Microsoft® Lync™ Server 2013

Survivable Branch Appliance

Mediant™ 1000B SBA

SBA Installation Manual

Mediant 1000B SBA for Microsoft Lync Server 2013

Version 6.6

February 2013

Document #: LTRT-40105

Microsoft® Lync™

Microsoft Partner
Gold Unified Communications

AudioCodes

Table of Contents

List of Figures

List of Tables

Reader's Notes

Notice

This document describes how to install and configure the Mediant 1000B Survivable Branch Appliance (SBA), located at the remote branch office and deployed in the Microsoft Lync Server 2013 environment.

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee the accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document and other documents, as well as software files can be viewed by registered customers at http://www.audiocodes.com/downloads.

Date Published: February-18-2013

Trademarks

AudioCodes, AC, AudioCoded, Ardito, CTI2, CTI², CTI Squared, HD VoIP, HD VoIP Sounds Better, InTouch, IPmedia, Mediant, MediaPack, NetCoder, Netrake, Nuera, Open Solutions Network, OSN, Stretto, TrunkPack, VMAS, VoicePacketizer, VoIPerfect, VoIPerfectHD, What's Inside Matters, Your Gateway To VoIP and 3GX are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and service are generally provided by AudioCodes' Distributors, Partners, and Resellers from whom the product was purchased. For technical support for products purchased directly from AudioCodes, or for customers subscribed to AudioCodes Customer Technical Support (ACTS), contact support@audiocodes.com.

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our Web site at http://www.audiocodes.com/downloads. Your valuable feedback is highly appreciated.

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

Related Documentation

Manual Name
Mediant 1000B SBA Quick Guide
Mediant 1000B SBA Software Upgrade and Recovery for Microsoft Lync Server 2013 Configuration Note
Mediant 1000B Hardware Upgrade for Microsoft Lync Server Configuration Note
AudioCodes Enhanced Gateway with Analog Devices for Microsoft Lync Server 2013 Configuration Note
Mediant E-SBC SIP Trunking for Microsoft Lync 2013 Configuration Note

1 Introduction

This document provides step-by-step instructions on installing and configuring the Survivable Branch Appliance (SBA) application running on AudioCodes Mediant 1000B OSN3, located at the remote branch office and deployed in the Microsoft Lync Server 2013 environment. The Mediant 1000B SBA includes an OSN Server platform with Windows Server 2008 R2 operating system, and with preinstalled Lync Server 2013 Registrar and Mediation Server software installation (MSI), and a PSTN gateway, all in a single appliance chassis.

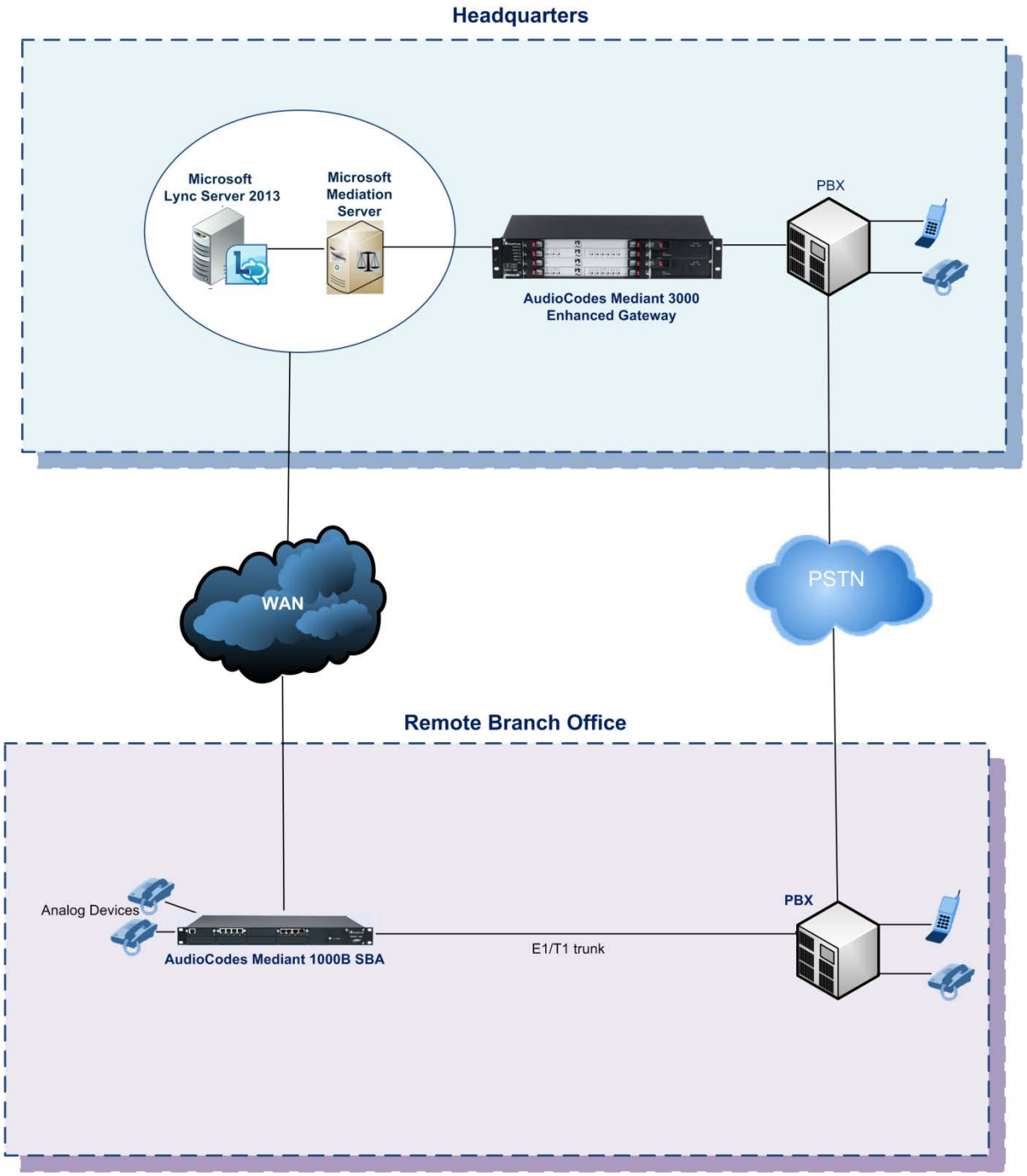
In the Lync Server 2013 environment, given the centralized deployment model, Unified Communication (UC) users in a remote site are dependent on the servers in the enterprise's data center (typically at headquarters) for their communication, and hence are vulnerable to losing communication capabilities when the WAN is unavailable. Given the always-available expectation for voice, it is imperative that the UC solution continues to provide the ability for branch users to make and receive calls when the WAN from the branch to the primary data center is unavailable.

To provide voice services to branch users during a WAN outage, a branch office survivability solution–the Survivable Branch Appliance (SBA) application–is hosted on the OSN Server platform running on AudioCodes Mediant 1000B SBA located at the branch office. During a WAN connectivity failure, Mediant 1000B SBA maintains call connectivity among Microsoft users located at the branch office–Lync Server 2013 clients (for example, Microsoft Lync clients) and devices (for example, IP phones)–and between these users and the public switched telephone network (PSTN).

The AudioCodes Mediant 1000B gateway can also provide the Lync Server environment with a connection to Analog Devices. The Analog Devices are connected to the Mediant 1000B Foreign eXchange Station (FXS) port interfaces. This document provides also instructions on how to configure the gateway to use its internal FXS port as Analog Devices.

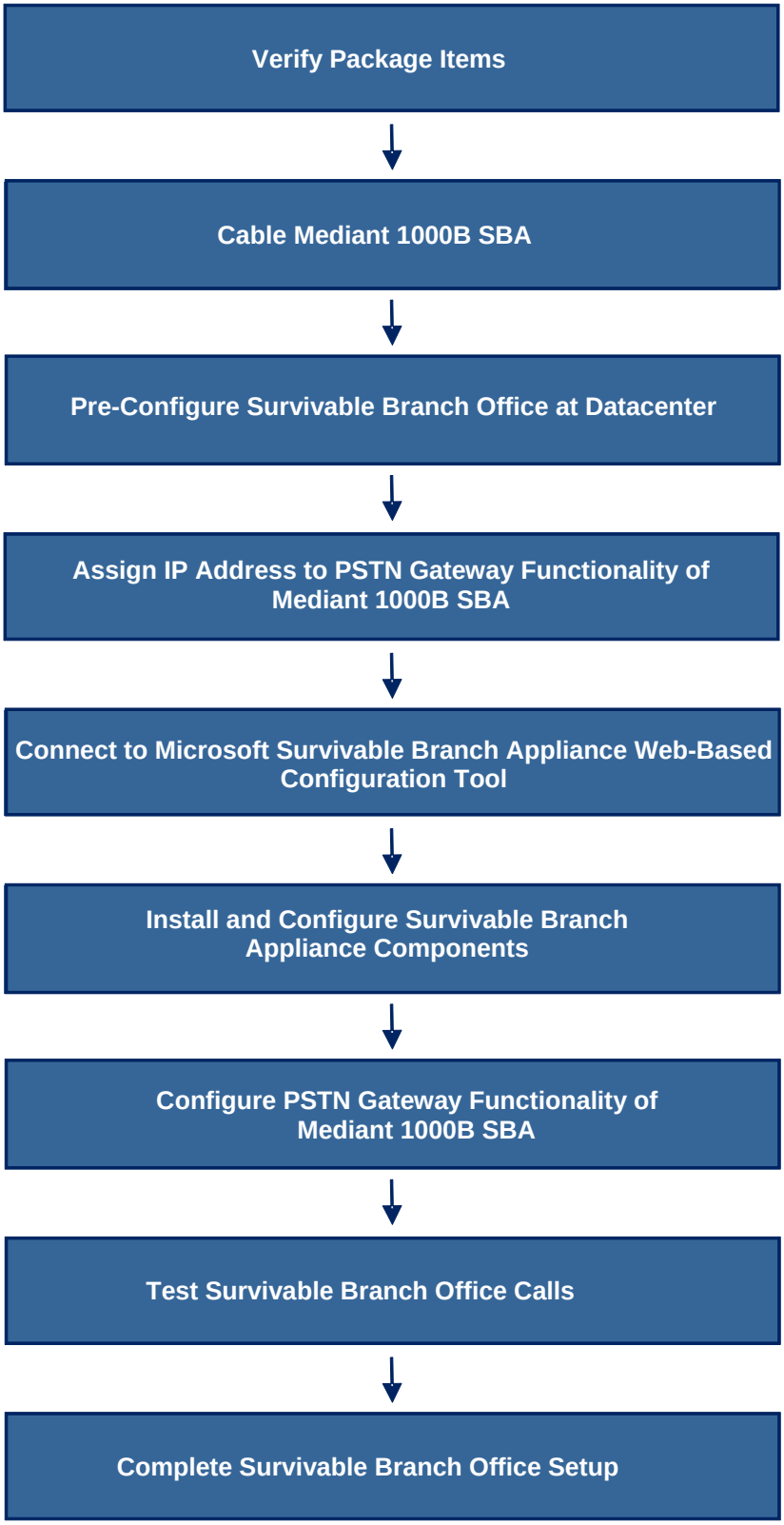
The figure below illustrates the integration of the Mediant 1000B SBA in the Lync Server 2013 environment.

Figure 1-1: Mediant 1000B SBA in Microsoft Lync Server 2013 Environment



The summary of the steps required to install the Mediant 1000B SBA is shown in the figure below:

Figure 1-2: Summary of Steps for Installing and Configuring SBA



Reader's Notes

2 Verifying Package Contents

Ensure that your Mediant 1000B SBA package is shipped with the following items:

- Four anti-slide bumpers for desktop installation
- 19-inch rack mounting kit (two flanges and six screws)
- RS-232 serial cable adaptor for serial communication between the Mediant 1000B OSN3 functionality (flat connector) and a computer (red DB-9 connector)
- Two mounting brackets for 19-inch rack mounting
- One FXS Lifeline cable adapter (only for models with FXS interfaces)
- T1 WAN splitter cable (only for models with T1 WAN interface)
- One AC power cable
- USB tool for SBA software upgrade and recovery procedure
- Microsoft Windows 2008 license document (envelope)

Check, retain and process any documents. If any items are missing or damaged, please contact your AudioCodes sales representative.

Reader's Notes

3 Mediant 1000B SBA Hardware Description

This section provides a hardware description overview of the Mediant 1000B SBA and instructions on how to cable the Mediant 1000B SBA.

3.1 Front Panel

The Mediant 1000B SBA front panel is shown below and described in the subsequent table.

Figure 3-1: Mediant 1000B SBA Front Panel

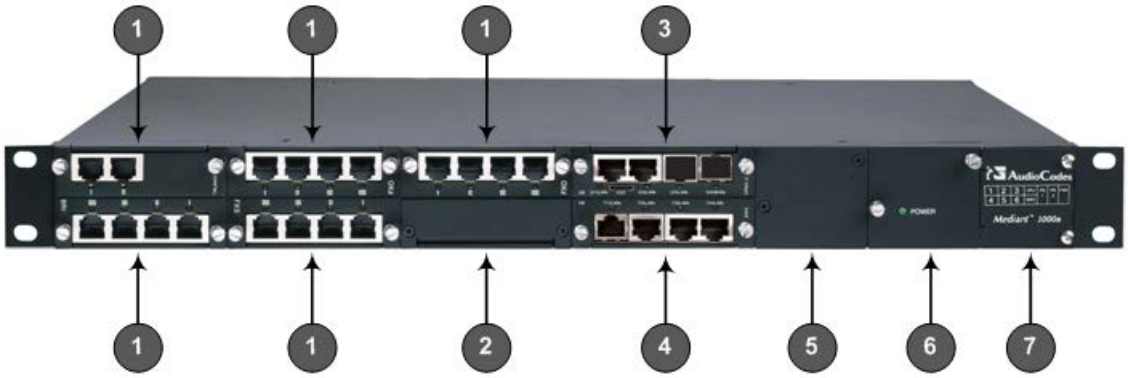


Table 3-1: Front-Panel Description

Item #	Label/ Module	Component Description
1	**FXS**	The FXS module provides the Foreign eXchange Subscriber (FXS) interfaces **Note:** The presence of this module depends on the ordered configuration. If in the future you need to add such interfaces to your device, you can order this module separately.
	FXO	The FXO module provides the Foreign eXchange Office (FXO) interfaces **Note:** The presence of this module depends on the ordered configuration. If in the future you need to add such interfaces to your device, you can order this module separately.
	BRI	The BRI module provides the Integrated Services Digital Network (ISDN), Basic Rate Interface (BRI) interfaces. **Note:** The presence of this module depends on the ordered configuration. If in the future you need to add such interfaces to your device, you can order this module separately.
	TRUNKS	TRUNKS (E1/TE/J1) module **Note:** The presence of this module depends on the ordered configuration. If in the future you need to add such interfaces to your device, you can order this module separately.

Item #	Label/ Module	Component Description
2	**MPM**	MPM module - The device supports up to three MPMs for IP media server capabilities (i.e., conferencing, SBC, and IP-to-IP routing applications). Depending on required configuration, the MPM module can be housed in chassis slots 3, 4, 5, or 6. **Note:** The presence of this module depends on the ordered configuration. If in the future you need to add such interfaces to your device, you can order this module separately.
3	**CRMX**	CRMX module - The CRMX module provides LAN interfaces (providing port-pair redundancy), an RS-232 interface, and a reset pinhole button.
4	**SWX**	LAN Extension (SWX) module – The SWX LAN Expansion module provides four LAN ports. These ports provide port-pair (group) redundancy, where one port is active and the other redundant**.** **Note:** The presence of this module depends on the ordered configuration. If in the future you need to add such interfaces to your device, you can order this module separately.
5	**Power 1**	(Optional) Spare Power Supply module slot. The device can provide two extractable power supply units (Power 1 and Power 2). Each power supply unit provides an AC power connector on its rear panel. If both Power 1 and Power 2 units are used, the load is shared between them. This (optional) load-sharing feature enables power failure protection (redundancy). When using this feature, you are advised to connect each power supply unit to a different AC supply circuit.
6	**Power 2**	Main Power Supply module.
7	**Schematic**	Extractable Fan Tray module with a schematic displayed on its front panel showing the chassis' slot numbers. The Fan Tray module cools the device's components.

3.2 Rear Panel

The Mediant 1000B SBA rear panel is shown below and described in the subsequent table.

Figure 3-2: Mediant 1000B SBA Rear Panel Showing OSN3 Server

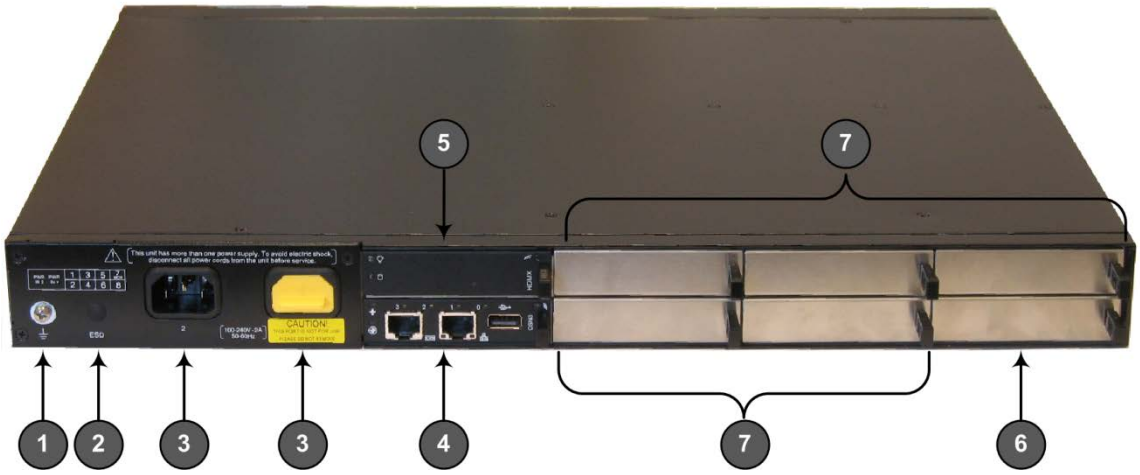


Table 3-2: Rear-Panel Description

Item #	Label	Description
1	⏚	Protective earthing screw.
2	ESD	Electrostatic Discharge (ESD) socket.
3	100-240V~1A	Dual AC Power Supply Entries.
4	OSN3	OSN3 AMC module.
5	HDMX	Main hard-disk drive (HDD) AMC module for OSN3 platform.
6	HDMX	Slot for second (optional) HDD for OSN3 platform.
7	-	Unused and covered AMC module slots.

3.3 OSN3 Platform

The OSN3 platform, on which the SBA is installed, consists of the following modules:

- OSN3 - see Section 3.3.1 on page 22
- HDMX - see Section 3.3.2 on page 27

3.3.1 OSN3 Module

The OSN3 module provides the port connector interfaces and is housed in Slot #2 on the Mediant 1000B SBA rear panel. The table below lists the OSN3 module specifications:

Table 3-3: OSN3 Module Specifications

Parameter	Specification
CPU	Intel® Core™ 2 Duo 1.5 GHz processors L7400 with Intel 3100 Chipset (64-bit)
RAM Memory	2 GB or 4 G DDR2 with ECC
Hard Drives	Up to 2 hard drives (HDMX modules)
Bus/Chipset	64 Bit
L2 Cache	2 M
Interfaces	▪ Gigabit Ethernet ▪ USB 2.0 via Connection Module ▪ RS-232 COM

The OSN3 module is shown below and described in the subsequent table.

Figure 3-3: OSN3 Module Ports

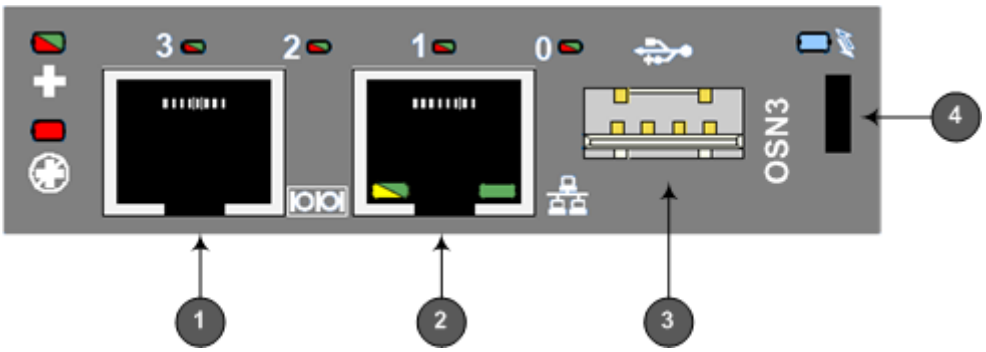


Table 3-4: OSN3 Module Port Description

Item #	Label	Description
1		RJ-45 port for RS-232 serial interface (COM1).
2		RJ-45 port for Gigabit Ethernet. The interface provides automatic detection and switching between 10Base-T, 100Base-TX and 1000Base-T data transmission (Auto-Negotiation). Auto-wire switching for crossed cables is also supported (Auto-MDI/X).
3		USB 2.0 port.
4	-	Handle for inserting and extraction module from slot.

3.3.1.1 LED Description

The OSN3 module LEDs are shown in the figure below and described in the subsequent table.

Figure 3-4: OSN3 Module LEDs

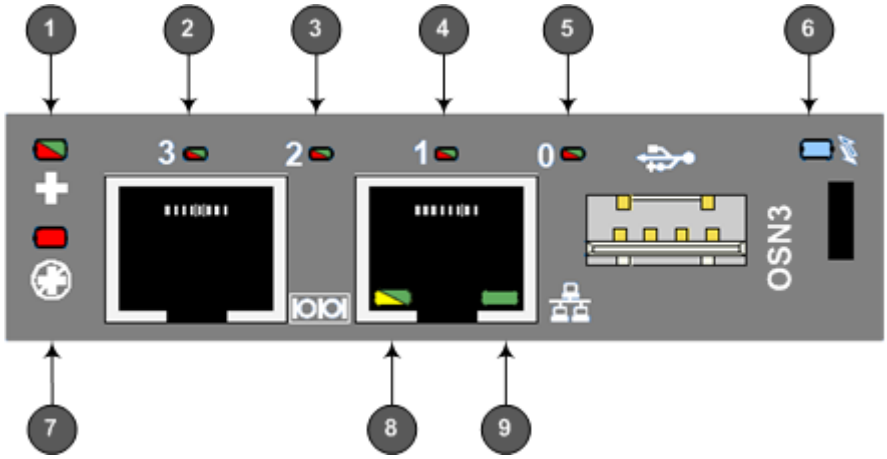


Table 3-5: OSN3 Module LEDs Description

Item	Label	Color	State	Description
1	+	**Green**	Flashing	Hardware normal operation.
		Red	On	Hardware fault (over-temperature or excess voltage feed).
2	**3**	**Red**	On	When lit during boot-up, indicates power failure.
			Flashing	Processor over-temperature above 100°C. If LEDs 0, 1, and 2 are also flashing, there is a processor over-temperature above 125°C and as a result, the module shuts down.
		-	Off	Normal operation.

Item	Label	Color	State	Description
3	**2**	**Red**	On	When lit during boot-up, indicates clock failure.
			Flashing	Chipset over-temperature above 105°C. If LEDs 0, 1, and 3 are also flashing, there is a processor over-temperature above 125°C and as a result, the module shuts down.
		-	Off	Normal operation.
4	**1**	**Red**	On	When lit during boot-up, indicates a hardware reset.
			Flashing	Processor over-temperature above 125°C and as a result, OSN3 shuts down (if LEDs 0, 2, and 3 are also flashing)
		-	Off	Normal operation.
5	**0**	**Red**	On	When lit up during boot-up, indicates a BIOS boot failure.
			Flashing	Processor over-temperature above 125°C and as a result, OSN3 shuts down (if LEDs 1, 2, and 3 are also flashing)
		-	Off	Normal operation.
6		**Blue**	Flashing	Module undergoing shutdown sequence when module pulled out to first extraction position.
			On	Module shutdown sequence complete and the module can be extracted from the chassis slot.
			Off	Module correctly inserted in chassis slot.
7		**Red**	On	Hardware failure (supplied voltage is not within normal operating range – ensure CRMX is installed in chassis).
			Flashing	Upgrade in progress.
		-	Off	Normal operation.
8	**SPEED**	**Green**	On	100Base-TX connection.
		Yellow	On	1000Base-T connection.
		-	Off	10Base-T connection if ACT LED active.
9	**ACT**	**Green**	On	Valid Ethernet link (cable connection) has been established.
		-	Off	The LED goes temporarily off if network packets are sent or received. When this LED remains off, a valid link has not been established due to a missing or a faulty cable connection.

3.3.1.2 Gigabit Ethernet Cable Connector Pinouts

The RJ-45 connector pinouts for the Gigabit Ethernet interface are listed in the table below:

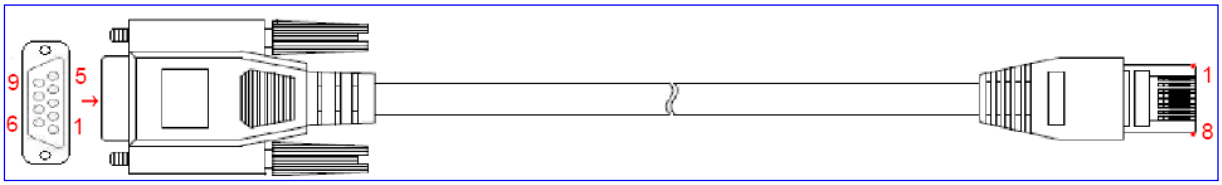
Table 3-6: Gigabit Ethernet Interface (RJ-45) Connector Pinouts

Pin	100Base-Tx		1000Base-T	
	I/O	Signal	Signal	Function
1	O	Tx+	I/O	BI_DA+
2	0	Tx-	I/O	BI_DA-
3	I	Rx+	I/O	BI_DB+
4			I/O	BI_DC+
5			I/O	BI_DC-
6	**I**	Rx-	I/O	BI_DB-
7			I/O	BI_DD+
8			I/O	BI_DD-

3.3.1.3 Serial Cable Connector Pinouts

The RJ-45-to-DB-9 female cable adapter is used for serial cabling.

Figure 3-5: RJ-45-to-DB-9 Serial Cable Adapter



The cable connector pinouts are listed in the table below:

Table 3-7: RS-232 Serial Cable Connector Pinouts

RJ-45	DB-9
1	8
2	6
3	2
4	5
5	5
6	3
7	4
8	7

3.3.2 HDMX (Hard-Disk Drive) Module

The HDMX module provides the hard-disk drive functionality for the OSN3 platform, providing storage capacity of 160 GB. This module is housed in Slot #1 on the Mediant 1000B SBA rear panel.

Notes:

- For additional storage capacity per HDMX module, contact your AudioCodes representative.
- The OSN3 can optionally be ordered with dual hard-disk drives (i.e., two HDMX modules).

The HDMX module is shown below and described in the subsequent table.

Figure 3-6: HDMX Module

Table 3-8: HDMX Module LED Description

Item #	Label	Color	State	Description
1		Green	On	Power received by module.
		-	Off	No power received by module.
2		Blue	On	Module can be extracted from chassis slot once dismounted from the OSN3 operating system.
			Off	Module correctly inserted in chassis slot
1		Red	On	Hard disk drive in use (active).
		-	Off	Hard disk drive not in use.

3.3.2.1 Inserting and Extracting OSN3 Modules

The OSN3 modules are hot-swappable and can be inserted and extracted without disrupting other non-related OSN3 services running on the Mediant 1000B SBA. In addition, if two HDMX modules are used and one needs to be replaced or removed, this can also be done without affecting OSN3 functionality. Therefore, you can remove and replace faulty modules without taking the entire Mediant 1000B SBA out of service (i.e., powering down).

The modules provide a handle that allows you to easily insert or extract them, as described in the subsequent subsections.

3.3.2.1.1 Inserting a Module

The procedure below describes how to insert a module into the chassis slot.

➢ **To insert a module:**

1. Carefully insert the module into the slot until it makes contact with the AMC card-edge connector located on the backplane.
2. Connect all external interfacing cables to the module, as required.
3. Using the module handle, engage the module with the chassis backplane.
4. When the handle is locked, the module is engaged and the **HS** LED turns off.

3.3.2.1.2 Removing an AMC Module

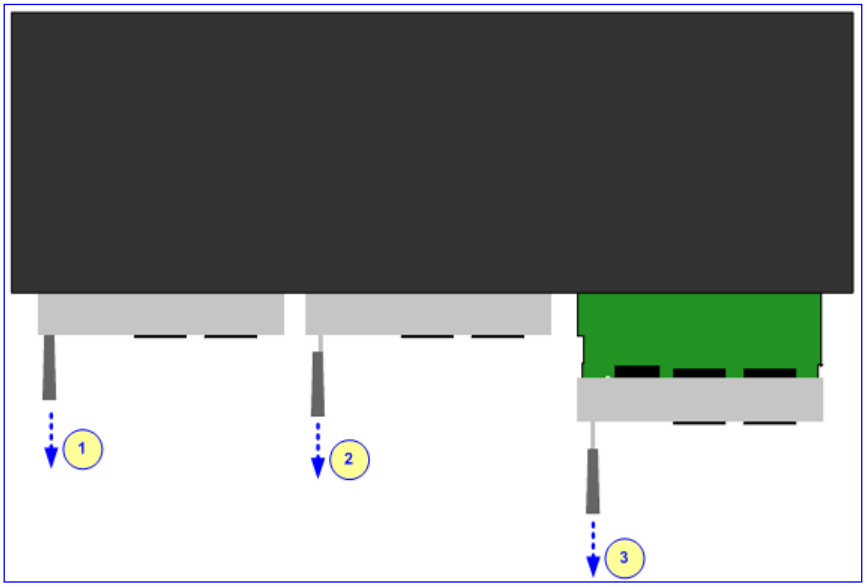
The procedure below describes how to remove a module from the chassis.

Note: Before removing the AMC module (if required), you must perform a hard-disk drive dismount (i.e., a logical disconnection of the hard drive).

➢ **To remove a module:**

1. Pull on the module handle and partially remove the module to the first "click"; the module performs a shutdown sequence, which is indicated by the flashing blue **Hot Swap** LED (see Stages 1 and 2 in the figure below).
2. When the LED stops flashing and remains constantly on, disconnect any cables that may be connected to the module.
3. Using the module handle, pull the module out of the slot (see Stage 3 in the figure below).

Figure 3-7: Removing AMC Modules



3.4 Cabling

This section describes how to cable the device:

- **Grounding the Device** – see Section 3.5 on page 30
- **Connecting to the LAN** – see Section 3.6 on page 30
- **Connecting to FXS interfaces** – see Section 3.7 on page 33
- **Connecting to BRI lines** – see Section 3.8 on page 34
- **Connecting to E1/T1 trunks** – see Section 3.9 on page 36
- **Connecting the PSTN Fallback for E1/T1 Trunks** – see Section 3.9.2 on page 37
- **Connecting the RS-232 Serial Interface to a Computer** – see Section 3.10 on page 38
- **Connecting to Power** – see Section 3.11 on page 39.

3.5 Grounding the Device

The procedure below describes how to ground the device.

Protective Earthing

The equipment is classified as Class I EN 60950 and UL 60950 and must be earthed at all times (using an equipment-earthing conductor).

- Finland: "Laite on liltettava suojamaadoituskoskettimilla varustettuun pistorasiaan."
- Norway: "Apparatet rna tilkoples jordet stikkontakt."
- Sweden: "Apparaten skall anslutas till jordat uttag."

➢ **To ground the device:**

1. Connect an electrically earthed strap of 16 AWG wire (minimum) to the chassis' earthing screw (located on the rear panel), using the supplied washer.

Figure 3-8: Grounding the Device

2. Connect the other end of the strap to a protective earthing. This should be in accordance with the regulations enforced in the country in which the device is installed.

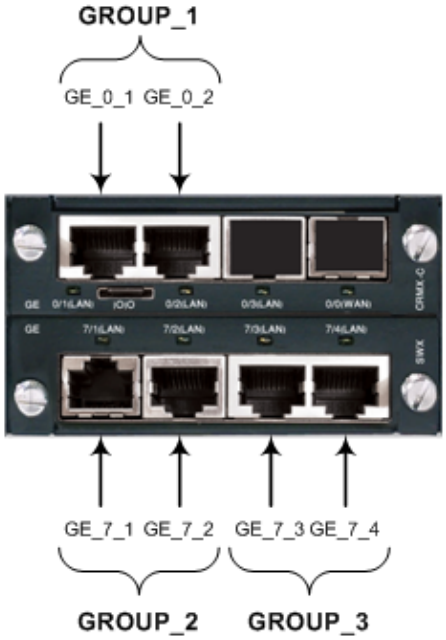
3.6 Connecting to LAN with Port-Pair Redundancy

The LAN ports are provided on the CRMX and SWX LAN Expansion modules. These LAN ports operate in pairs (*groups*) to provide LAN port 1+1 redundancy. In each pair, one port serves as the active LAN port while the other as standby. When the active port fails, the device switches to the standby LAN port.

Note: The SWX module is a customer ordered item.

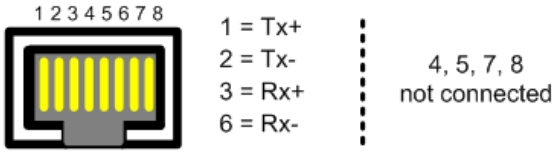
The figure below shows the LAN port-pair groups and the name of the ports and groups as displayed in the Web interface for configuring the port groups and assigning them to IP network interfaces (refer to the *User's Manual* for more information):

Figure 3-9: LAN Port-Pair Groups and Web Interface String Names



An RJ-45 cable connector with the following pinouts is used:

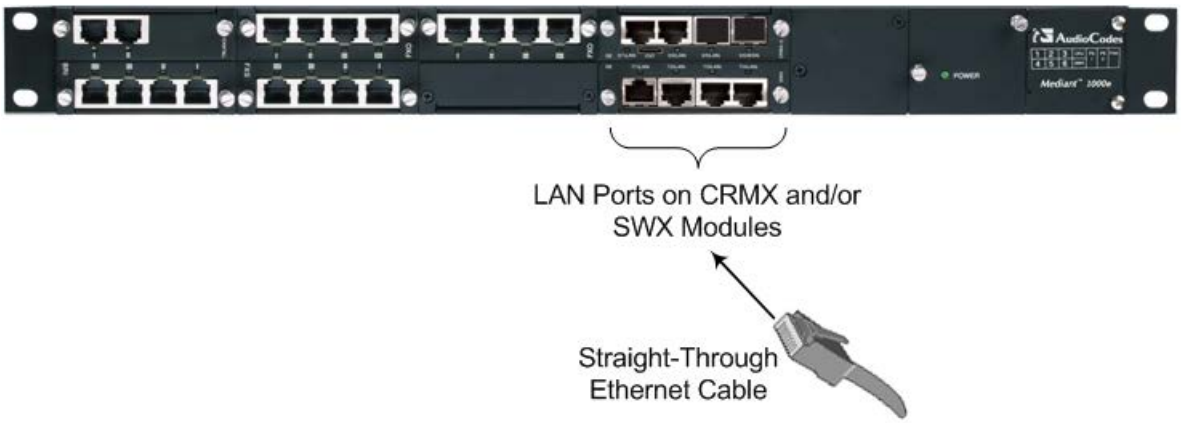
Figure 3-10: RJ-45 Connector Pinouts for LAN



➢ **To connect to the LAN:**

1. Connect one end of a straight-through RJ-45 Ethernet Cat 5/5e cable to the active LAN port on the CRMX or SWX module.

Figure 3-11: Connecting to LAN



2. Connect the other end of the cable to the LAN.
3. For 1+1 LAN protection, repeat Steps 1 and 2 for the standby port, but connect it to another network (in the same subnet).

Note: If you are implementing the LAN port-pair redundancy, ensure that the two ports making up a pair are each connected to a different network (in the same subnet).

3.7 Connecting to FXS Interfaces

The procedure below describes how to connect to FXS interfaces such as fax machines, modems, and plain old telephone system (POTS) telephones.

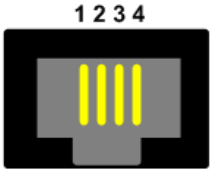
Warnings:

- Ensure that FXS ports are connected to the appropriate external devices; otherwise, damage to the device may occur.
- The FXS ports are considered as TNV-2..

Note: The FXS module is a customer ordered item. This section is applicable only if your device is installed with such a module.

An RJ-11 cable connector with the following pinouts is used:

Figure 3-12: RJ-11 Connector Pinouts for FXS



1 - Not connected
2 - Tip
3 - Ring
4 - Not connected

➢ **To connect to FXS interfaces:**

- Using an RJ-11 connector, connect the FXS port/s to the required telephone interface.

3.8 Connecting to ISDN BRI Interfaces

This section describes how to connect to the ISDN BRI Interfaces.

3.8.1 Connecting to BRI Lines

The procedure below describes how to connect to BRI lines.

Warning: To protect against electrical shock and fire, use a 26 AWG min wire to connect the BRI ports to the PSTN.

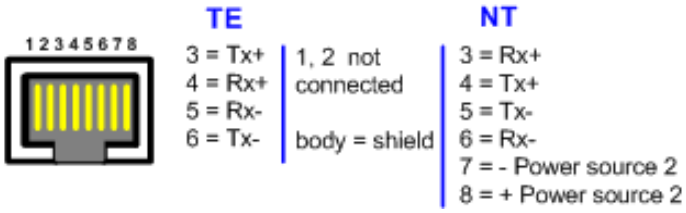
Note: The BRI module is a customer ordered item. This section is applicable only if your device is installed with such a module.

➢ **To connect to BRI lines:**

1. Connect the BRI cable to the device's BRI RJ-45 port.
2. Connect the other end of the cable to your ISDN telephone or PBX/PSTN switch.

A BRI port can be configured either as TE (Termination Equipment/user side) or NT (Network Termination/network side). The connector pinouts vary according to the configuration, as shown below:

Figure 3-13: RJ-45 Connector Pinouts for BRI



When configured as NT, the BRI port drives a nominal voltage of 38 V with limited current supply of up to 100 mA. The voltage is of Power Source 1 type (line voltage). Power Source 2 is optional.

3.8.2 Connecting the PSTN Fallback for BRI Lines

The device supports a PSTN Fallback feature for BRI lines, whereby if a power outage or IP connectivity problem (e.g., no ping) occurs, IP calls are re-routed to the PSTN. This guarantees call continuity.

PSTN Fallback is supported if the device houses one or more BRI modules, where each BRI module provides two or four spans.

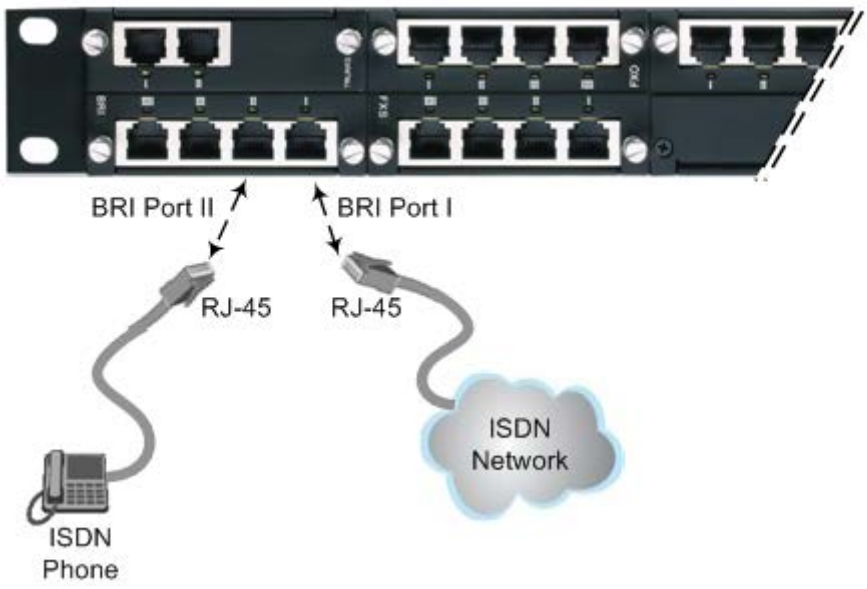
In the event of a PSTN fallback, the BRI module's metallic relay switch automatically connects line Port 1 (**I**) to Port 2 (**II**), and / or line Port 3 (**III**) to Port 4 (**IIII**) of the same BRI module.

For example, if a PBX trunk is connected to Port 1 and the PSTN network is connected to Port 2, when PSTN Fallback is activated, calls from the PBX are routed directly to the PSTN through Port 2.

➢ **To connect the BRI line interfaces for 1+1 PSTN Fallback:**

1. Connect Line 1 to a PBX.
2. On the same BRI module, connect Line 2 to the PSTN.

Figure 3-14: Cabling (Ports 1 and 2) PSTN Fallback



Notes:

- PSTN Fallback is supported only on the BRI module.
- PSTN Fallback is supported only between ports on the same BRI module.
- The scenarios that trigger PSTN Fallback (i.e., power outage and/or IP network loss) are configured by the *TrunkLifeLineType* parameter. For more information, see the *User's Manual*.
- This PSTN Fallback feature has no relation to the PSTN Fallback Software Upgrade Key

3.9 Connecting to ISDN E1/T1 Interfaces

This section describes how to connect to ISDN E1/T1 Interfaces.

3.9.1 Connecting to E1/T1 Trunks

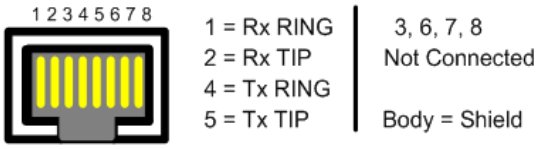
The procedure below describes how to connect to E1/T1 trunks.

Warning: To protect against electrical shock and fire, use a 26 AWG min wire to connect T1 or E1 ports to the PSTN.

Note: The TRUNKS module is a customer ordered item. This section is applicable only if your device is installed with such a module.

An RJ-48c trunk cable connector with the following pinouts is used:

Figure 3-15: RJ-48c Connector Pinouts for E1/T1



➢ **To connect to E1/T1l trunks:**

1. Connect the E1/T1 trunk cables to the ports on the device's TRUNKS module(s).
2. Connect the other ends of the trunk cables to a PBX/PSTN switch.

3.9.2 Connecting the PSTN Fallback for E1/T1 Trunks

The device supports a PSTN Fallback feature, whereby upon a power outage or IP connectivity problem (e.g., no ping), IP calls are re-routed to the PSTN. This guarantees call continuity.

PSTN Fallback is supported if the device houses one or two E1/T1 ("TRUNKS") modules, where each module provides two or four spans. In the event of a PSTN fallback, the module's metallic relay switch automatically connects trunk Port 1 (**I**) to Port 2 (**II**), and / or trunk Port 3 (**III**) to Port 4 (**IIII**) of the same module. For example, if a PBX trunk is connected to Port 1 and the PSTN network is connected to Port 2, when PSTN Fallback is activated, calls from the PBX are routed directly to the PSTN through Port 2.

➢ **To connect the digital trunk interfaces for 1+1 PSTN Fallback:**

1. Connect Trunk 1 to a PBX.
2. On the same TRUNKS module, connect Trunk 2 to the PSTN.

Figure 3-16: Cabling (Ports 1 and 2) PSTN Fallback

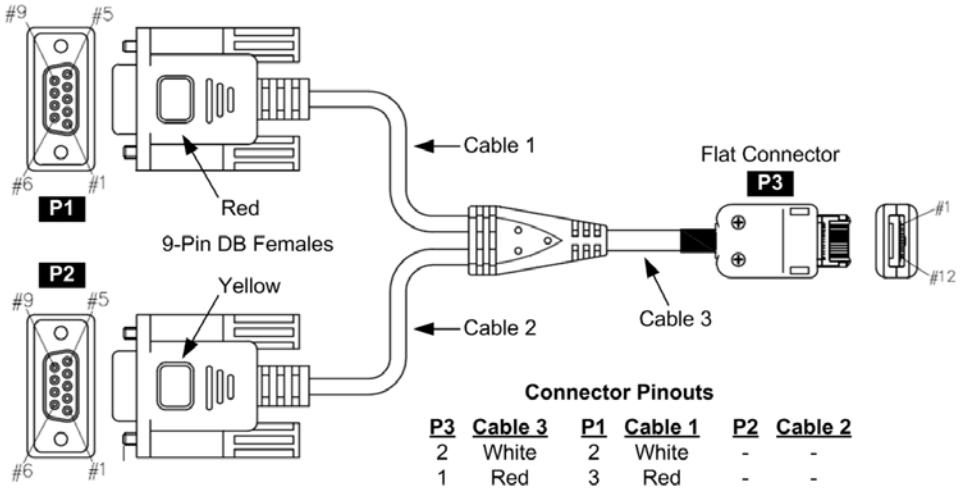
Notes:

- PSTN Fallback is supported only on the TRUNKS module.
- PSTN Fallback is supported only between ports on the same TRUNKS module.
- PSTN Fallback is supported only for ISDN when the number of supported channels (e.g., 30) is less than the maximum number of possible channels provided by the physical ports (e.g., two E1 trunks). When the number of supported channels (e.g., 60) equals the maximum number of channels provided by the physical ports (e.g., two E1 trunks), then other protocols such as CAS are also supported.
- The scenarios (i.e., power outage and/or IP network loss) upon which PSTN Fallback is triggered is configured by the *TrunkLifeLineType* parameter. For more information, see the *User's Manual*.
- This PSTN Fallback feature has no relation to the PSTN Fallback Software Upgrade Key.

3.10 Connecting the RS-232 Serial Interface to a Computer

The device's RS-232 interface port is used to access the CLI for serial communication. The cable adapter shown below is provided for this purpose:

Figure 3-17: RS-232 Cable Adapter



Connector Pinouts

P3	Cable 3	P1	Cable 1	P2	Cable 2
2	White	2	White	-	-
1	Red	3	Red	-	-
4	Brown	-	-	2	White
3	Black	-	-	3	Red
8	Orange	5	Black	-	-
9	Yellow	-	-	5	Black

➢ **To connect the serial interface port to a computer:**

1. Connect the flat connector (labeled "P3" in the figure above) to the serial port (labeled **1010**) on the device's CRMX module.
2. Connect the DB-9 connector labeled "P1" (red) to the COM1 or COM2 RS-232 communication port of your computer.

Notes:

- The RS-232 port is not intended for permanent connection.
- The DB-9 connector labeled "P2" is used only for debugging.

3.11 Connecting to Power

The procedure below describes how to connect the device to the AC power supply.

Warning:

- Units must be connected (by service personnel) to a socket-outlet with a protective earthing connection.
- Use only the AC power cord supplied with the device.

Notes:

- You can install up to two Power Supply modules (Power 1 and Power 2), each providing an AC power connector on the device's rear panel. The dual power option provides the device with power redundancy. If both power units are used (for load sharing - failure protection / redundancy), ensure that you connect each power supply unit to a different AC supply circuit.
- The two AC power sources must have the same ground potential.

➢ **To connect the device to the power supply:**

- On the device's rear panel, connect the left (active) 100-240V~50-60 Hz power socket to a standard electrical outlet using the supplied AC power cord.

When the device receives powers, the **POWER** LED on the front panel of the Power Supply module is lit green. If the LED is off, a power supply problem may be present.

Reader's Notes

4 Assigning IP Address to PSTN Gateway

The Mediant 1000B SBA includes an embedded Web server (*Web interface*), providing a user-friendly graphical user interface (GUI) for configuring PSTN gateway-related functionality (*PSTN Gateway*). The IP address used for accessing this Web interface must be changed to suit the networking scheme in which your Mediant 1000B SBA is deployed.

Before you can configure the PSTN Gateway, you need to first access it with the default VoIP / Management LAN IP address, as described in Section 4.1 below.

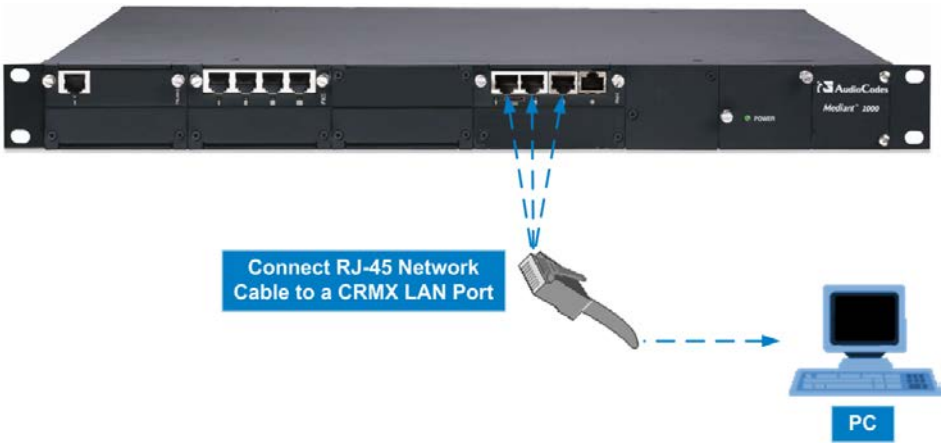
4.1 Initial Access to the PSTN Gateway

Before you can configure the PSTN Gateway, you need to access its Web interface using the default VoIP / Management LAN IP address, as described in below.

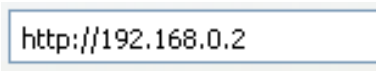
➢ **To initially access the PSTN Gateway:**

1. Connect one of the LAN ports on the CRMX module of the Mediant 1000B SBA directly to a PC, using a straight-through Ethernet cable.

Figure 4-1: Connecting Mediant 1000B SBA LAN Port on CRMX Module (Front Panel)

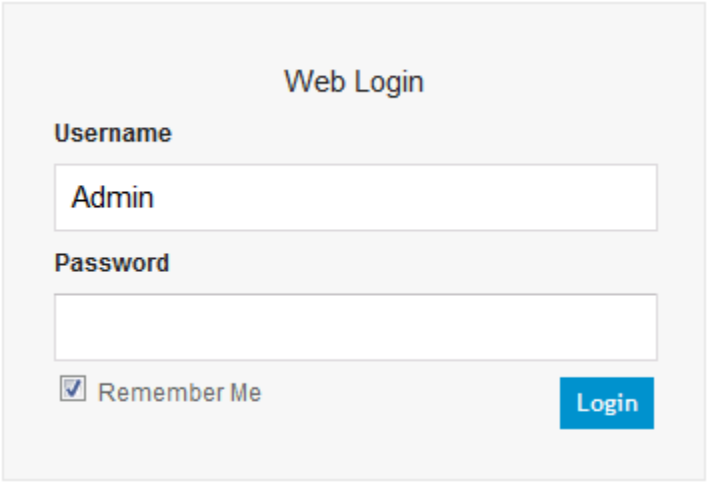


2. Change your computer's IP address so that it is on the same subnet as the default IP address (i.e., **192.168.0.3**) of the Mediant 1000B PSTN Gateway.
3. Open a standard Web browser, and then in the URL address field, enter the Mediant 1000B SBA default VoIP / Management LAN IP address (i.e., **192.168.0.2**):



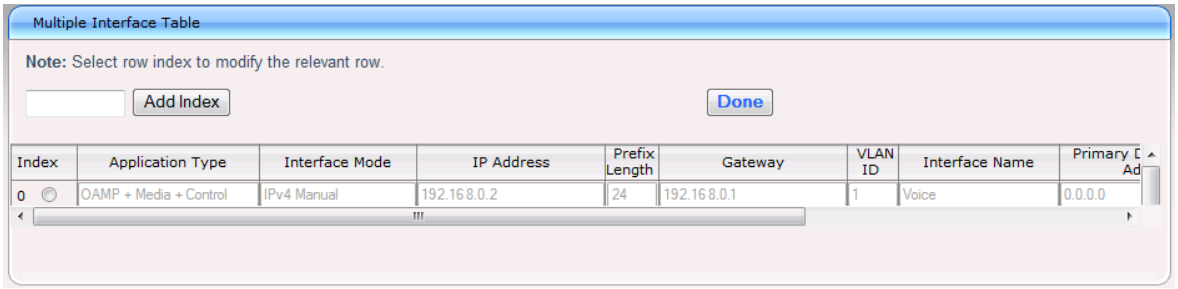
4. The following login screen appears, prompting you to log in with your login credentials:

Figure 4-2: Login Screen



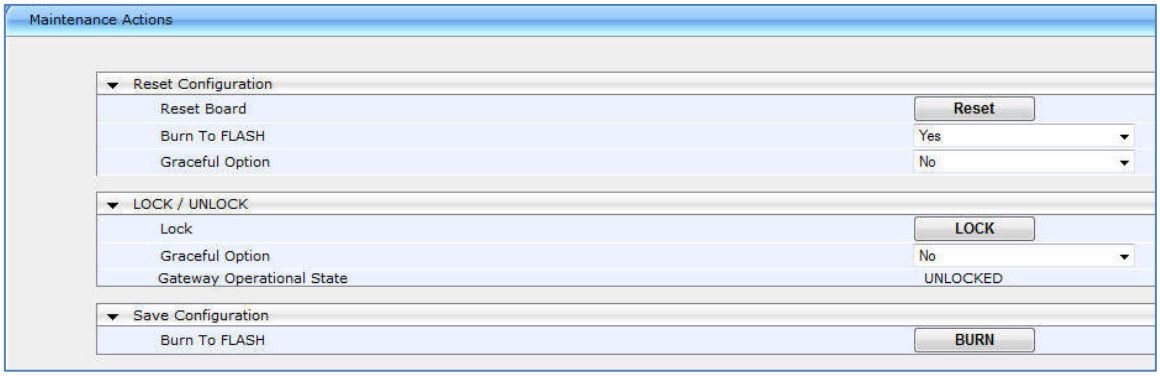
5. Log in with the default, case-sensitive user name ("Admin") and password ("Admin"), and then click **OK**; the Web interface appears, displaying the Home page.
6. Open the Physical Ports Settings page (**Configuration** tab > **VoIP** menu > **Network** > **Physical Ports Settings**) and then modify the device's physical Ethernet port-pair (group) that you want to later assign to the OAMP interface. For more information, see Section 4.2 on page 44.
7. Open the Multiple Interface Table page (**Configuration** tab > **VoIP** menu > **Network** > **IP Settings**), as shown below:

Figure 4-3: IP Settings Screen



8. Select the 'Index' radio button corresponding to the Application Type **OAMP + Media + Control"**(i.e., the VoIP and Management LAN interface), and then click **Edit.**
9. Configure a LAN network address so that it corresponds to your network IP addressing scheme.
10. From the 'Underlying Interface' drop-down list, select the physical LAN port-pair group that you want to assign to the interface.
11. Click **Apply**, and then click **Done** to apply and validate your settings.
12. On the toolbar, from the **Device Actions** drop-down list, choose **Reset**, and then in the' Maintenance Actions' page, click the **Reset** button; the Mediant 1000B resets and your settings are saved to the flash memory.

Figure 4-4: Maintenance Actions: Reset Gateway



13. Maintain the cabled connection between the Mediant 1000B LAN port and the computer.

4.2 Configuring Physical Ethernet Ports

The device's physical LAN ports are grouped into pairs (termed *Group Members*), where each group consists of an active port and a standby port. This provides LAN port redundancy within a group, whereby if an active port is disconnected and the other port is connected the device switches over to the standby port, making it active and the previously active port becomes non-active. These port groups can be assigned to IP network interfaces in the Multiple Interface table. Each port group can be assigned to up to 32 interfaces. This enables physical separation of network interfaces, providing a higher level of segregation of sub-networks. Equipment connected to different physical ports is not accessible to one another. The only connection between them can be established by cross connecting them with media streams (a VoIP calls).

For each LAN port, you can configure the speed, duplex mode, native VLAN (PVID), and provide a brief description. Up to three port-pair redundancy groups are supported, where one port-pair is on the CRMX module and two port-pairs are on the SWX LAN Expansion module.

➢ **To configure the physical Ethernet ports:**

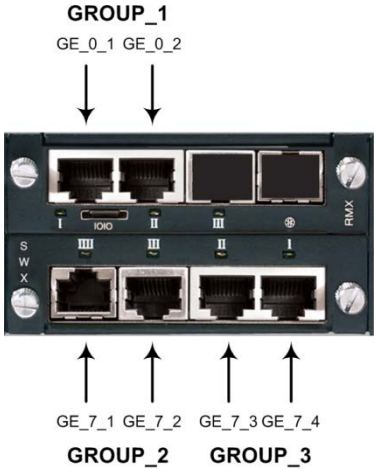
1. Open the Physical Ports Settings page (**Configuration** tab > **VoIP** menu > **Network** > **Physical Ports Settings**).

Figure 4-5: Physical Ports Settings Page

Index	Port	Mode	Native Vlan	Speed&Duplex	Description	Group Member	Group Status
1	GE_0_1	Enable	1	Auto Negotiation	User Port #0	GROUP_1	Redundant
2	GE_0_2	Enable	1	Auto Negotiation	User Port #1	GROUP_1	Redundant

2. Select the 'Index' radio button corresponding to the port that you want to configure.
3. Click the **Edit** button.
4. Configure the ports (see the table below for a description of the parameters).
5. Click **Apply**.

Table 4-1: Physical Port Settings Parameters Description

Parameter	Description
Port	(Read-only) Displays the port number. The string values displayed on the Web page represent the physical ports, as shown below: 

Parameter	Description
Mode	(Read-only field) Displays the mode of the port: ▪ **[0]** Disable ▪ **[1]** Enable (default)
Native Vlan	Defines the Native VLAN or PVID of the port. Incoming packets without a VLAN ID are tagged with this VLAN. For outgoing packets, if the VLAN ID as defined in the Multiple Interface table is the same as the Native VLAN ID, the device sends the packet without a VLAN; otherwise, the VLAN ID as defined in the Multiple Interface table takes precedence. The valid value range is 1 to 4096. The default is 1.
Speed & Duplex	Defines the speed and duplex mode of the port. ▪ **[0]** 10BaseT Half Duplex ▪ **[1]** 10BaseT Full Duplex ▪ **[2]** 100BaseT Half Duplex ▪ **[3]** 100BaseT Full Duplex ▪ **[4]** Auto Negotiation (default) ▪ **[6]** 1000BaseT Half Duplex ▪ **[7]** 1000BaseT Full Duplex
Description	Defines an arbitrary description of the port.
Group Member	(Read-only field) Displays the group to which the port belongs.
Group Status	(Read-only) Displays the status of the port: ▪ "Active" - the active port ▪ "Redundant" - the standby (redundant) port

Reader's Notes

5 Pre-Configuring SBA at Datacenter

Prior to installing the SBA at the branch office (as described later in Section 7 on page 63), you must perform the following at the datacenter (typically, located at headquarters):

- Add the SBA Device to the Active Directory (AD).
- Create a user account on the AD belonging to the **RTCUniversalSBATechnicians** group. This user performs the SBA deployment (Domain Admin account can also perform SBA deployment, by default).
- Add (publish) the SBA Device to your topology.

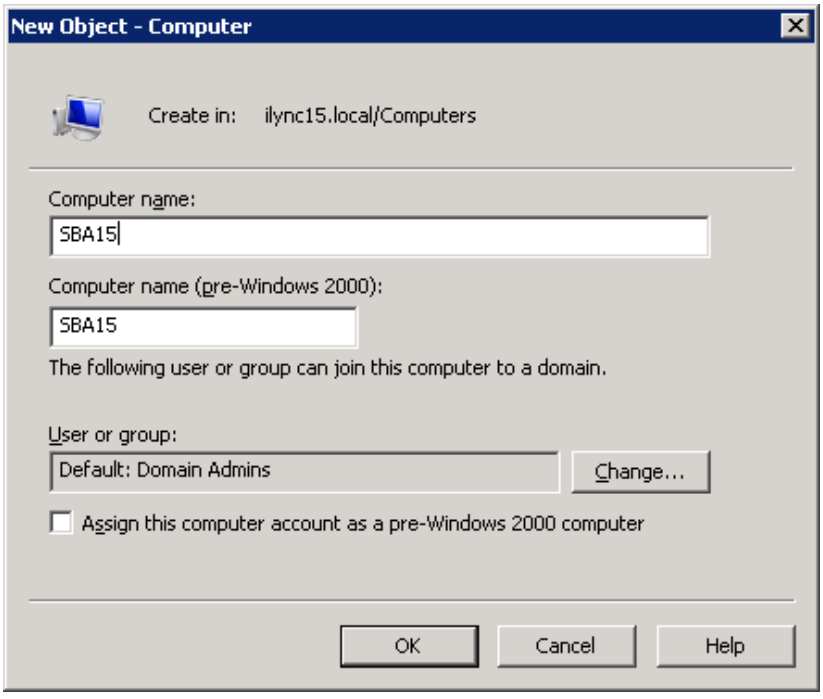
5.1 Adding the SBA Device to the Active Directory

The procedure below describes how to add the SBA device to the AD.

➢ **To add the SBA device to the Active Directory:**

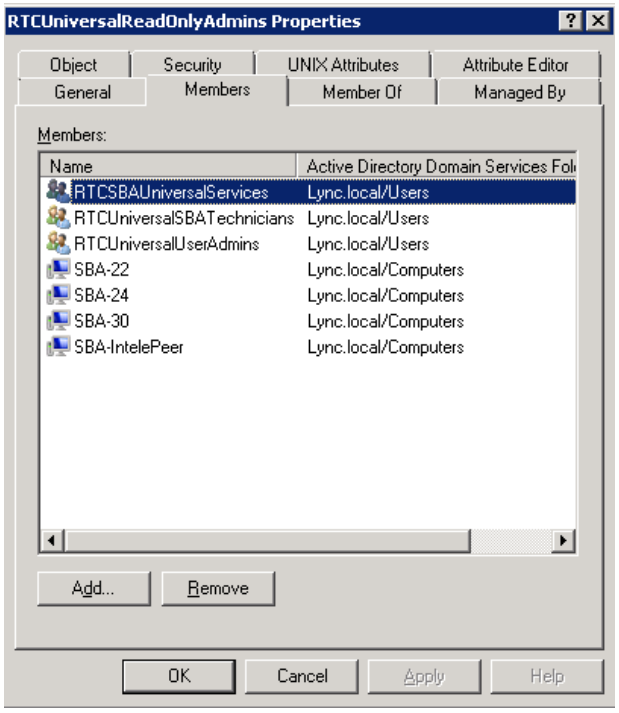
1. Add the planned Survivable Branch Appliance device name to the Active Directory Domain Services:
   a. Start the Active Directory Users and Computers program (**Start** > **Administrative Tools** > **Active Directory Users and Computers**).
   b. Add the Survivable Branch Appliance device name to the domain computers (right-click **Computers**, choose **New**, and then click **Computer**).

Figure 5-1: New Object – Computer Dialog Box



   c. Click **Change** to add a user or group that can insert this specific SBA server to the domain. (if you working with the Domain Administrator, do not change the "Domain Admin" group, if you working with another user, specify the name of a user or group that is allowed to join this computer to the domain.
   d. Add the Survivable Branch Appliance computer object to the **RTCUniversalReadOnlyAdmins** group (**Users > RTCUniversalReadOnlyAdmins** (right-click, select **Properties**, and then select the Numbers tab and **Add**).

Figure 5-2: RTCUniversalReadOnlyAdmins



e. Start the ADSI Edit program (**Start** > **Administrative Tools** > **ADSI Edit**).

f. Right-click the Survivable Branch Appliance computer name (that you created in Step 'b' above), and then choose **Properties**.

g. In the Attributes list, set **servicePrincipalName** to "HOST/<SBA FQDN>", where *SBA FQDN* is the FQDN of your Survivable Branch Appliance (e.g., HOST/SBA15.iLync15.local).

2. Create a user account on Active Directory Services belonging to the **RTCUniversalSBATechnicians** group. This user performs the Survivable Branch Appliance deployment.

5.2 Defining the Branch Office Topology using Topology Builder

This section describes how to add the Survivable Branch Appliance to your topology, using Lync Server 2013 Topology Builder. This configuration includes the following main steps:

- Defining the branch office – see Section 5.2.1 below
- Publishing the topology – see Section 5.2.2 on page 56

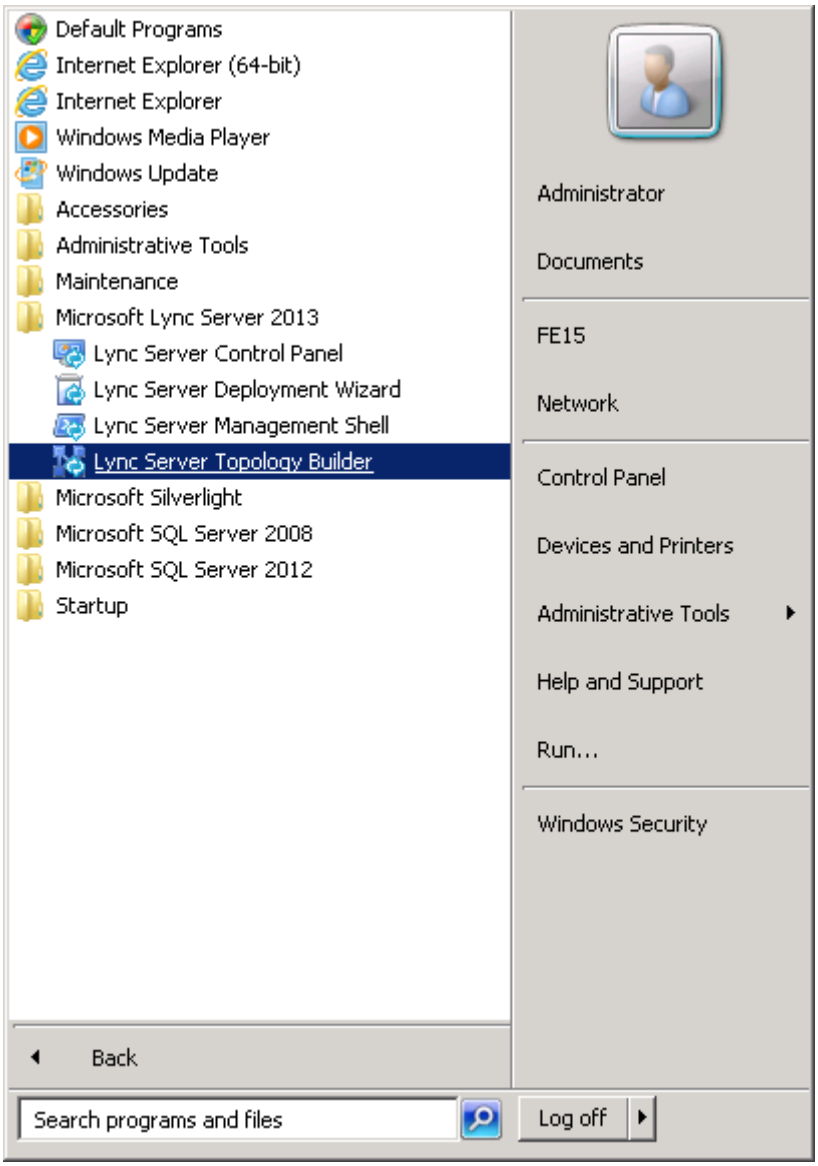
5.2.1 Defining the Branch Office

The procedure below describes how to create and define the branch office.

➢ **To create branch sites:**

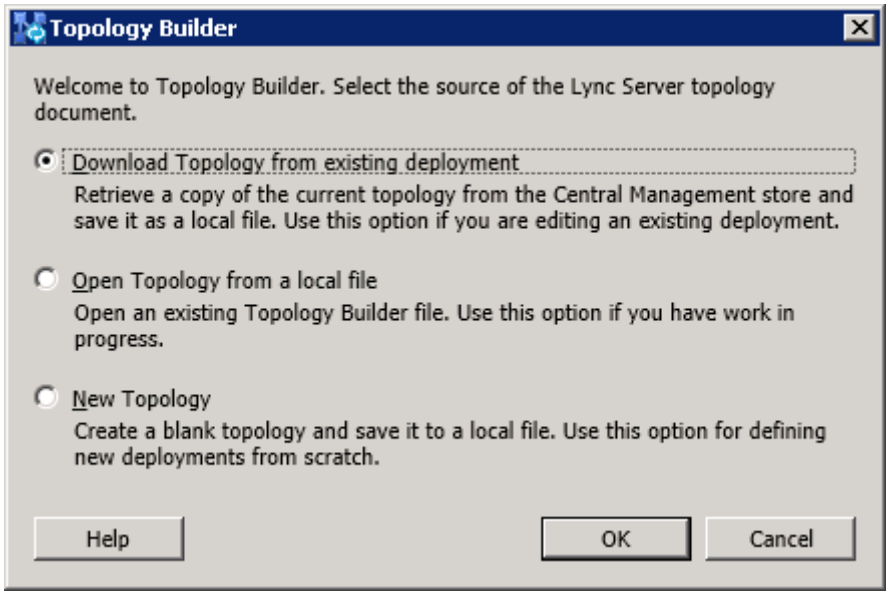
1. Start the Lync Server 2013 Topology Builder program (**Start** menu > **All Programs** > **Microsoft Lync Server 2013**, **Lync Server Topology Builder**), as shown below:

Figure 5-3: Menu Path to Topology Builder Program



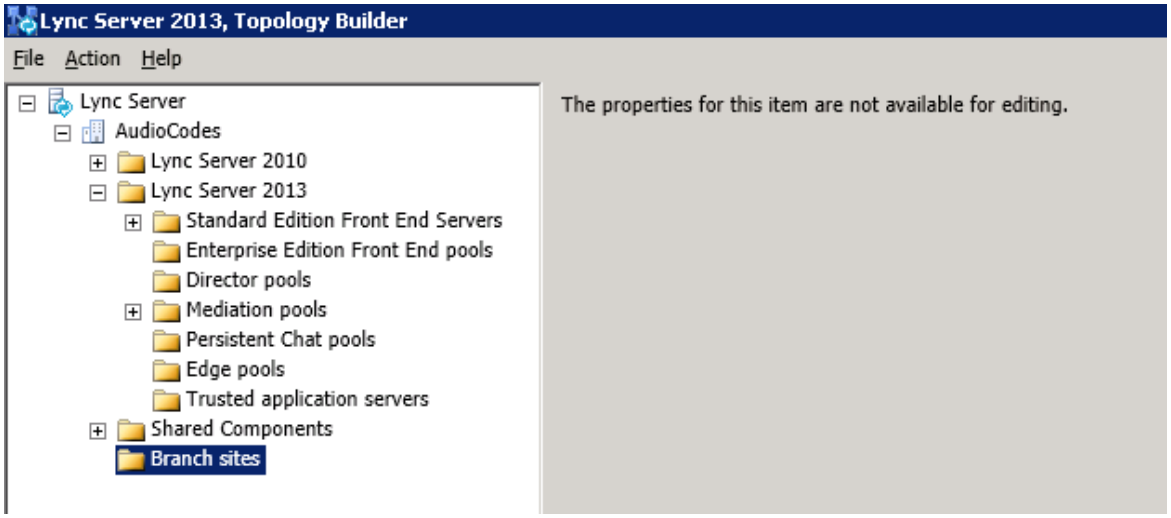
The Topology Builder opens, as shown below:

Figure 5-4: Topology Builder



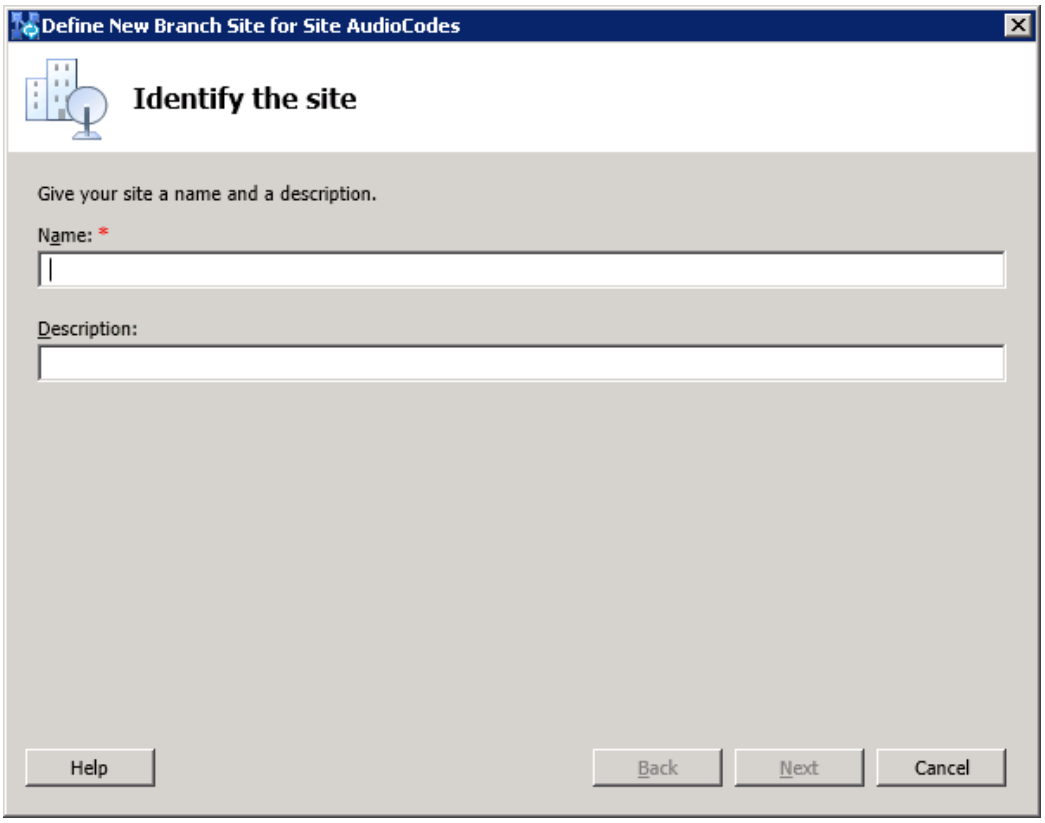
2. Select the **Download Topology from existing deployment** option (assuming your Lync Server 2013 deployment already has a topology), and then click **OK**; a dialog box opens, prompting you to save the existing topology file.
3. Save the topology; the following screen appears:

Figure 5-5: Lync Server 2013 Topology Builder



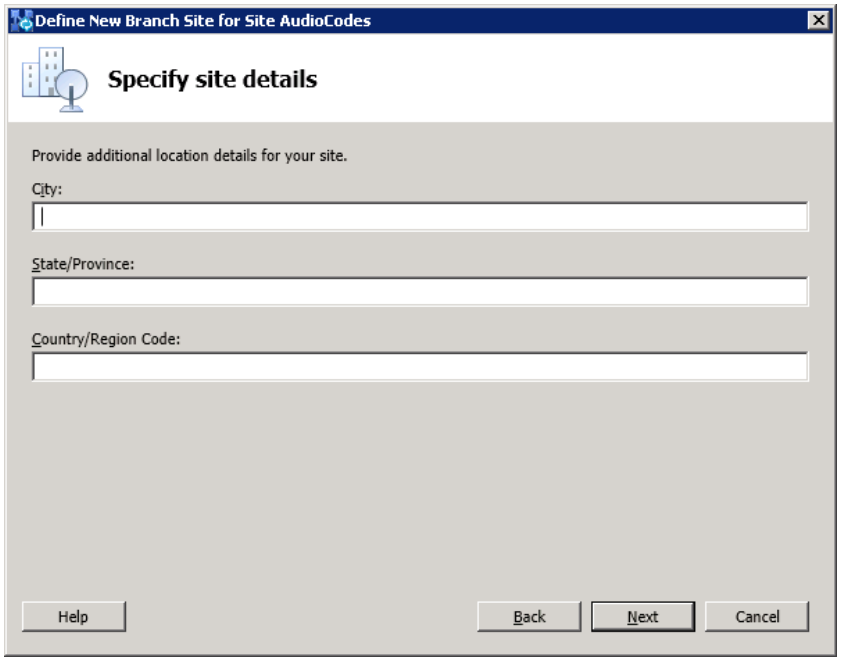
4. From the Topology Builder console tree, do one of the following:
   - If you used the Planning tool to design your Enterprise Voice topology, expand the **Branch sites** node, and then expand the name of the branch site you specified in the tool. To modify each section of the branch office, right-click the branch site, and then from the shortcut menu, choose **Edit Properties**.
   - If you did not use the Planning tool, right-click the **Branch sites** node, and then from the shortcut menu, choose **New Branch Site**; the following dialog box appears:

Figure 5-6: Identify the Site



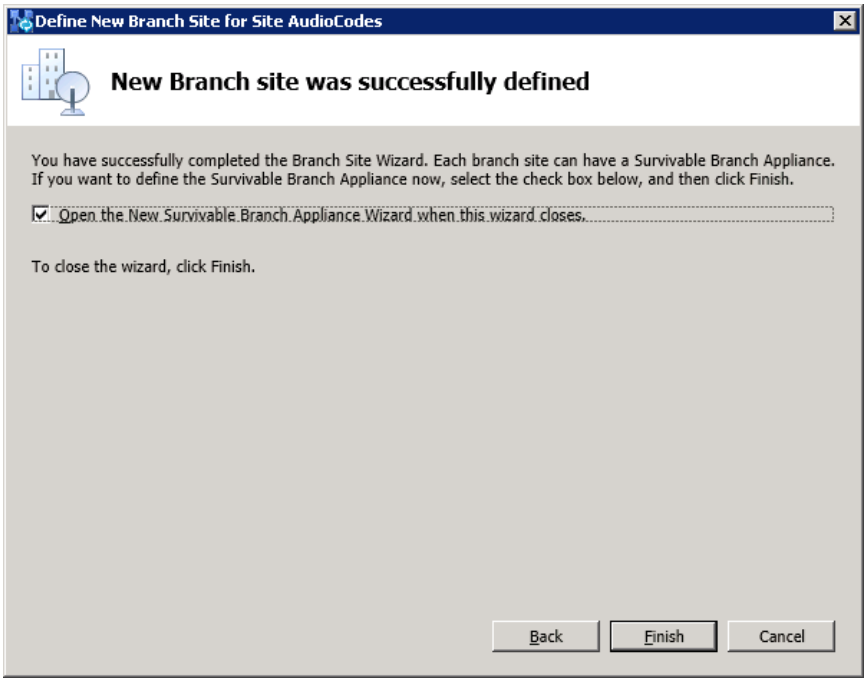
5. In the dialog box, do the following:
   a. In the 'Name' field, type the name of the branch site. Only this field is required, the other fields are optional.
   b. In the 'Description' field, type a meaningful description of the branch site.
   c. Click **Next**; the following dialog box appears:

Figure 5-7: Specify Site Details



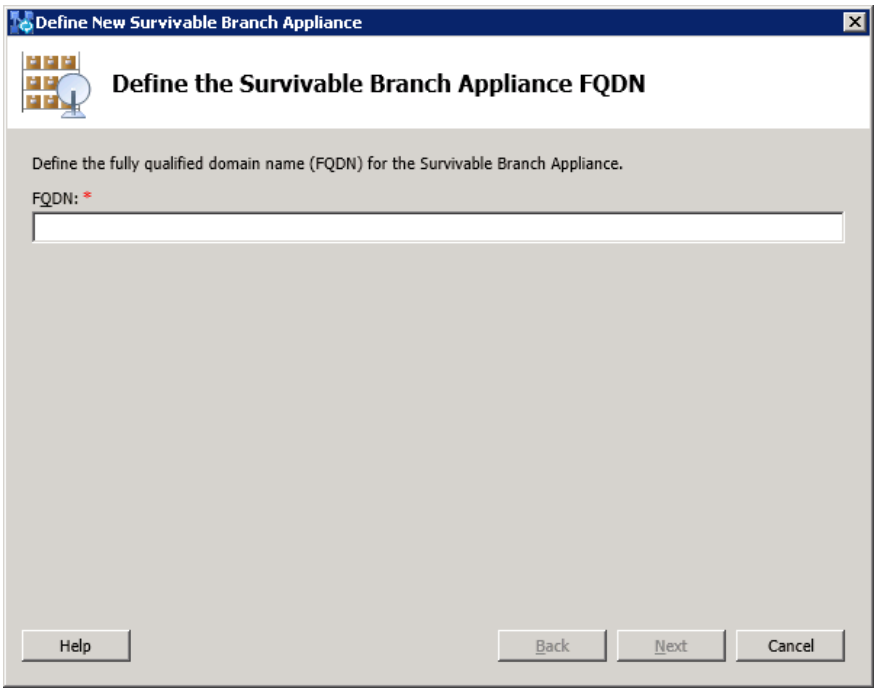
6. In the dialog box, do the following:
   a. In the 'City' field, type the name of the city in which the branch site is located.
   b. In the 'State/Province' field, type the name of the state or region in which the branch site is located.
   c. In the 'Country/Region Code' field, type the two-digit calling code for the country in which the branch site is located.
   d. Click **Next**; the following dialog box appears:

Figure 5-8: New Branch Site Successfully Defined



7. Select the check-box, **Open the New Survivable Branch Appliance Wizard when this wizard closes**, and then click **Finish**; the following dialog box appears:

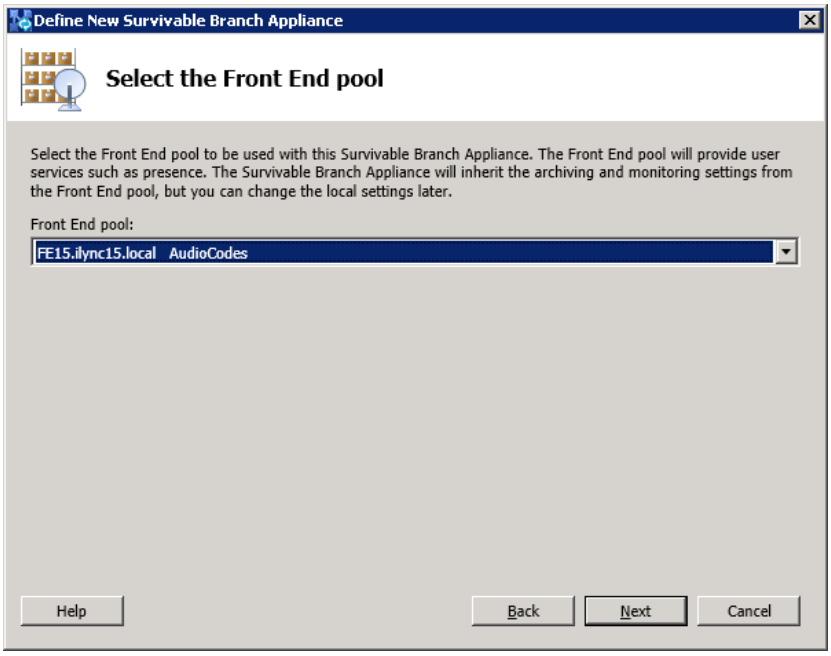
Figure 5-9: Define the Survivable Branch Appliance FQDN



8. In the 'FQDN' field**,** type the FQDN of the SBA, and then click **Next**; the following dialog box appears:

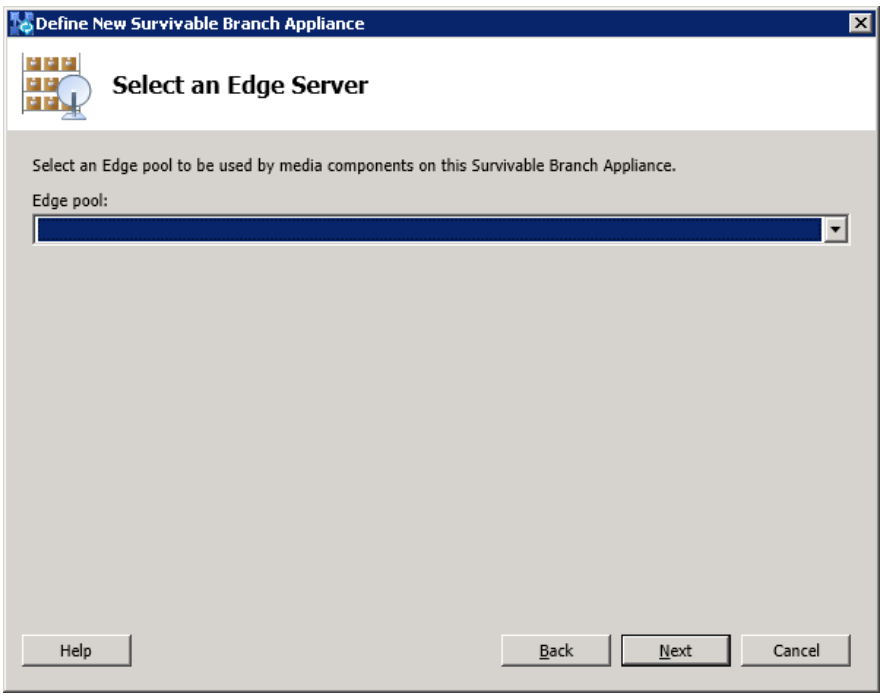
Note: The Survivable Branch Appliance FQDN that you configured in the 'FQDN' field must be the same as the FQDN that you configured using the ADSI Edit program in Section 5.1 on page 47.

Figure 5-10: Select the Front End Pool



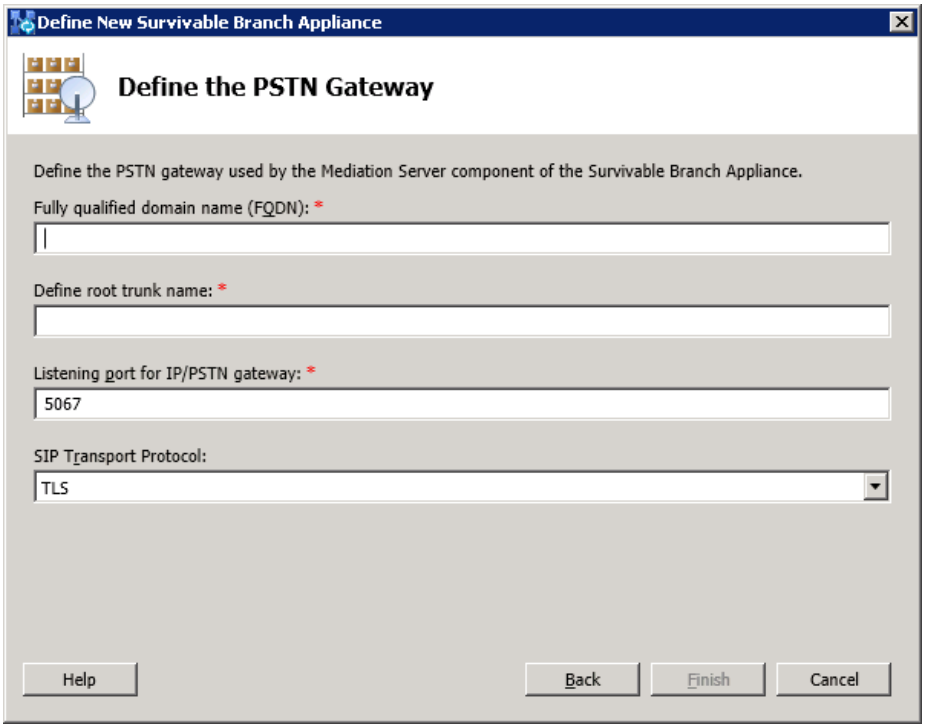
9. From the 'Front End pool' drop-down list, select the Front End pool to be used with this SBA, and then click **Next**; the following dialog box appears:

Figure 5-11: Select an Edge Server



10. From the 'Edge pool' drop-down list, select the Edge pool to be used with this SBA (optional), and then click **Next**; the following dialog box appears:

Figure 5-12: Define the PSTN Gateway



11. Do the following:

a. In the 'Gateway FQDN or IP Address' field, type the PSTN Gateway FQDN or IP address on which the Mediation Server component of the SBA is running. This is the IP address as configured for the PSTN Gateway. If you are using FQDN, ensure that your DNS server is configured to resolve the FQDN into this IP address.

b. In the 'Listening port for IP/PSTN Gateway' field, type the Gateway listening port. This must be the same port as configured in the PSTN Gateway, as described in Section 8.3 on page 106.

c. Under the **SIP Transport Protocol** group, select the **SIP Transport Protocol** option. This must be the same transport type as configured in the PSTN Gateway, as described in Section 8.3 on page 106.

Note: For call security, it is highly recommended that you deploy a Survivable Branch Appliance using TLS.

d. Click **Finish**.

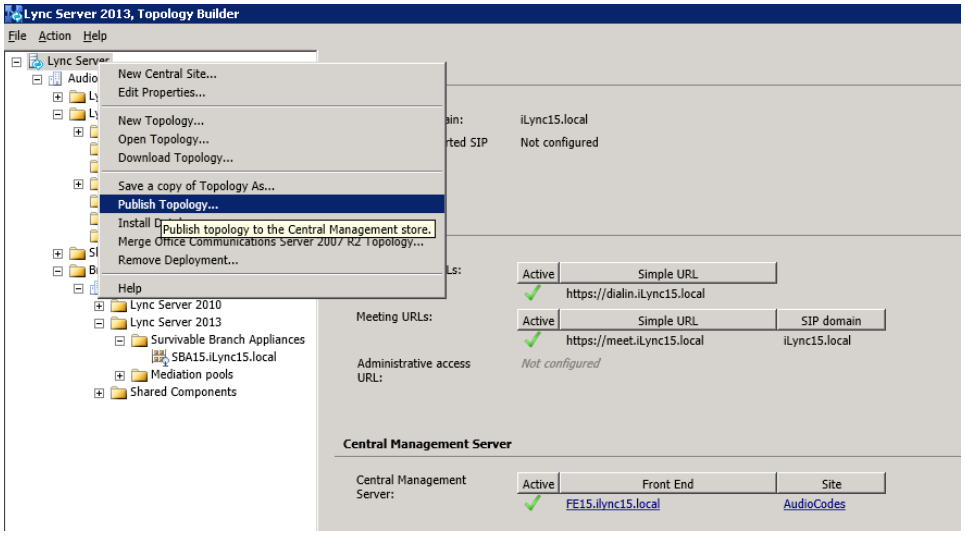
5.2.2 Publishing the Topology

Once you have defined the Branch Office (as described in the previous section), you need to publish this new topology, as described below.

➢ **To publish the topology:**

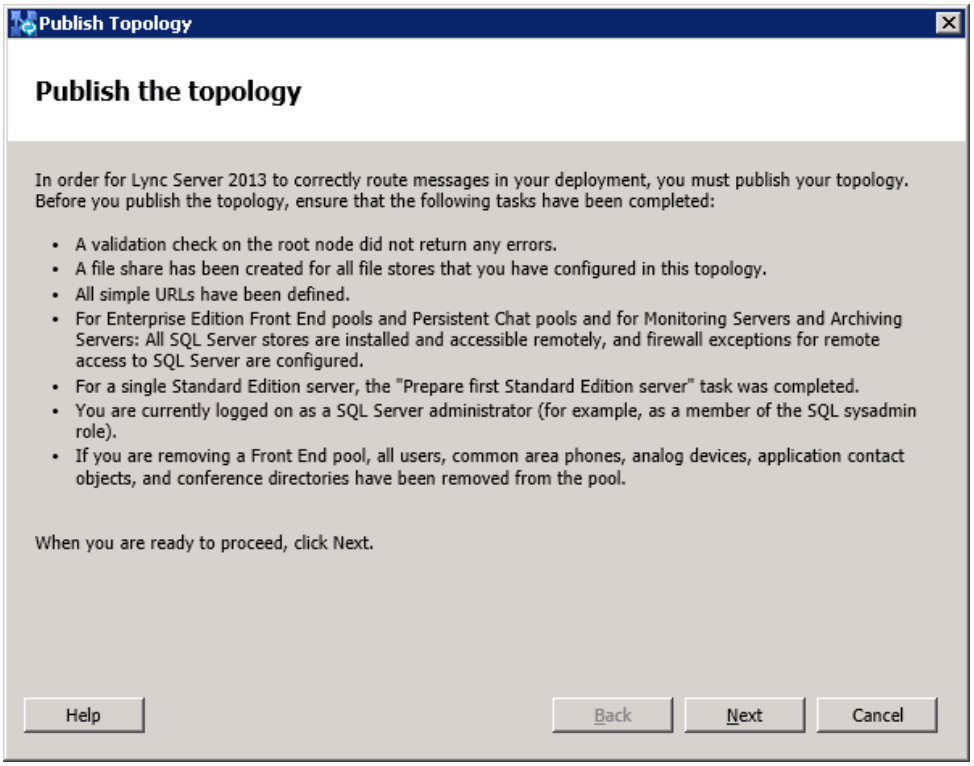
1. Right-click the root of the **Lync Server 2013** node, and then choose **Publish Topology**.

Figure 5-13: Publish Topology Selection



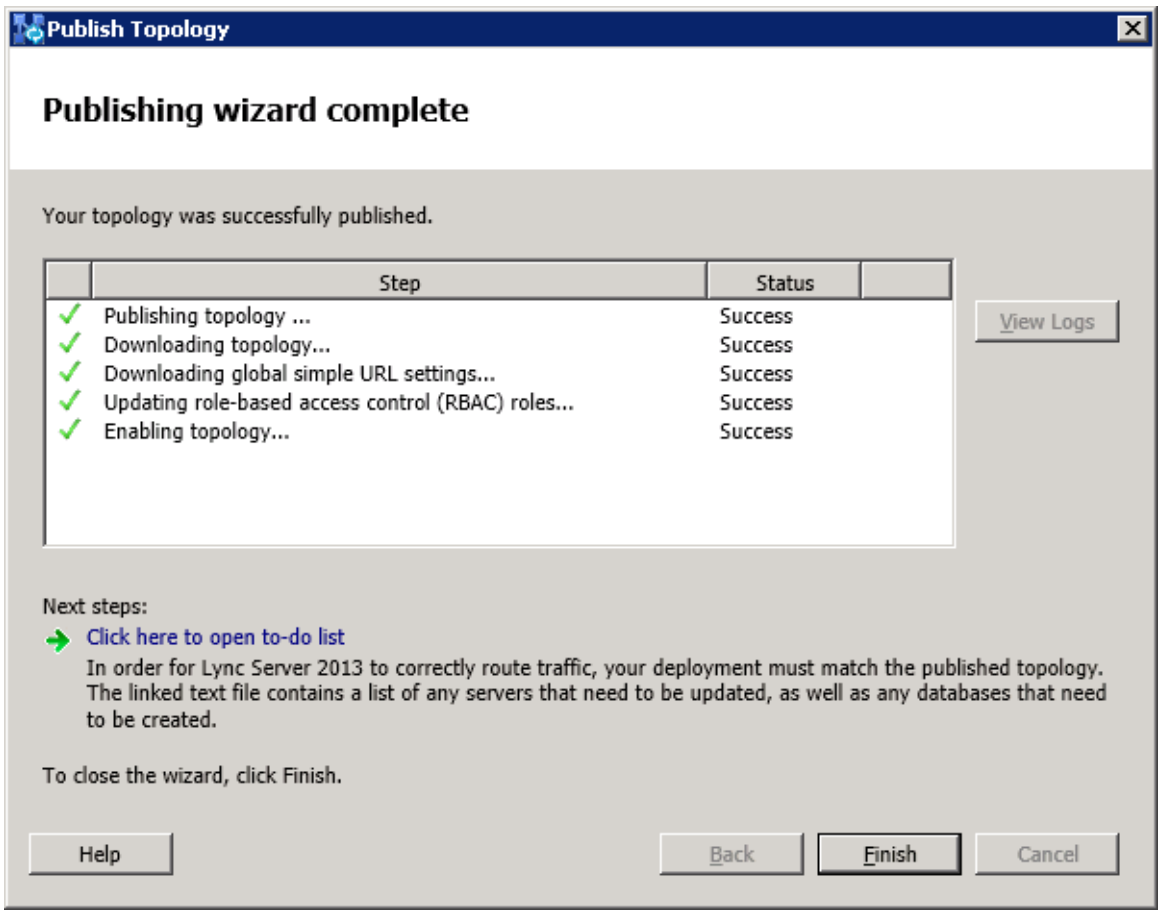
The following screen appears:

Figure 5-14: Publish the Topology



2. Click **Next**; the following screen appears:

Figure 5-15: Publish Wizard Complete



3. Verify that all steps display the 'Success' status, and then click **Finish**.

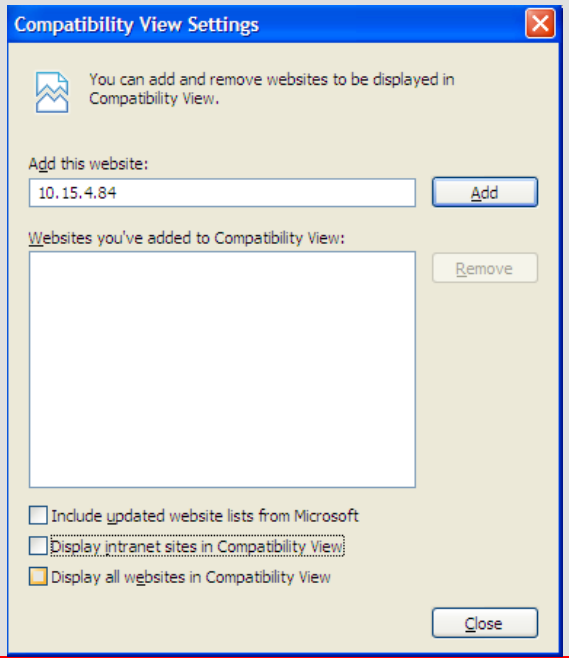
Reader's Notes

6 Connecting to the SBA Web-Based Tool

The SBA Web-based, graphical user interface (GUI) tool is used for installing and configuring the SBA application running on the Mediant 1000B SBA OSN3 server. You can connect and log in to the SBA Web-based tool using the default LAN IP address of the OSN3 server, or by using a different IP address that suites your environment, as described in Section 6.1 on page 60. (The IP address of the OSN3 server is synonymous with the IP address of the SBA.)

Note: The SBA Web-based tool is supported only by Internet Explorer 8 and higher (Compatibility disabled), Firefox, and Google Chrome.

Internet Explorer 8 compatibility can be disabled by selecting **Tools** > **Compatibility View Settings**. The **Display all websites in Compatibility View** check box must be unchecked (cleared). The SBA server must not appear in the list of "Websites you've added to Compatibility View".



6.1 Assigning an IP Address to SBA

The default IP address of the OSN3 server is 10.1.10.12/16, which is used to access the SBA Web-based tool. However, you can change this IP address to suit your network environment, using one of the following methods:

- SBA Web-based tool
- Serial connection

Note: If the SBA was recovered or upgraded using the AudioCodes Upgrade and Recovery USB tool, the IP address of the OSN3 server is received from the DHCP server and therefore, the default IP address (10.1.10.12) is no longer applicable.

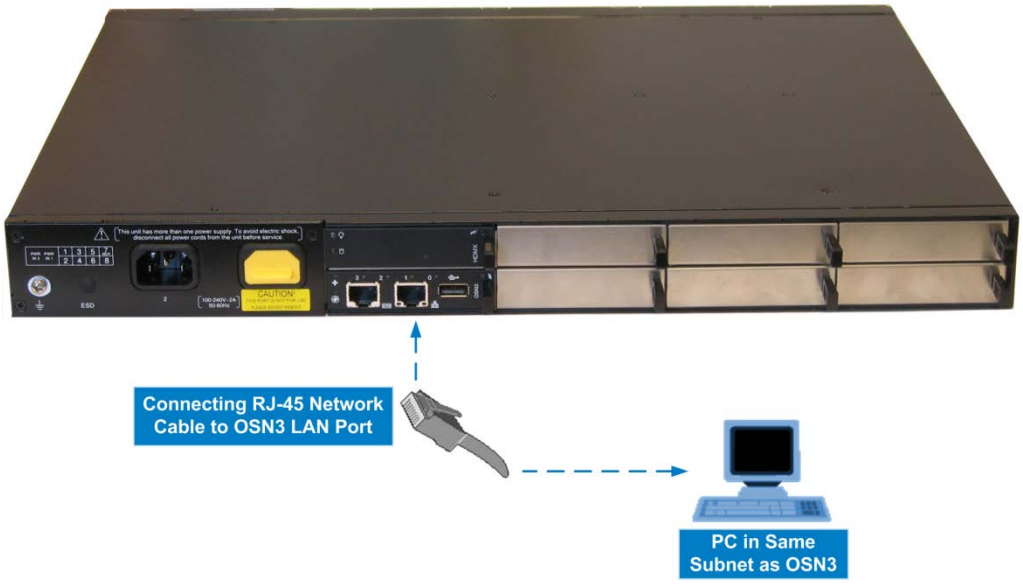
6.1.1 Using the SBA Web-Based Tool

You can assign an IP address to the SBA using the SBA Web-based tool, which is connected through the OSN3 LAN port.

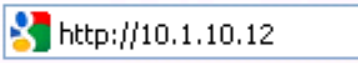
➢ **To change the IP address of the SBA:**

1. Change your computer's IP address so that it is in the same subnet as the default IP address (i.e., **10.1.10.15**) of the OSN3 server hosting the SBA.
2. Using a network cable, connect the computer to the LAN port on the Mediant 1000B SBA OSN3 module, as shown below:

Figure 6-1: Connecting to LAN Port on OSN3 Module (Rear Panel View)

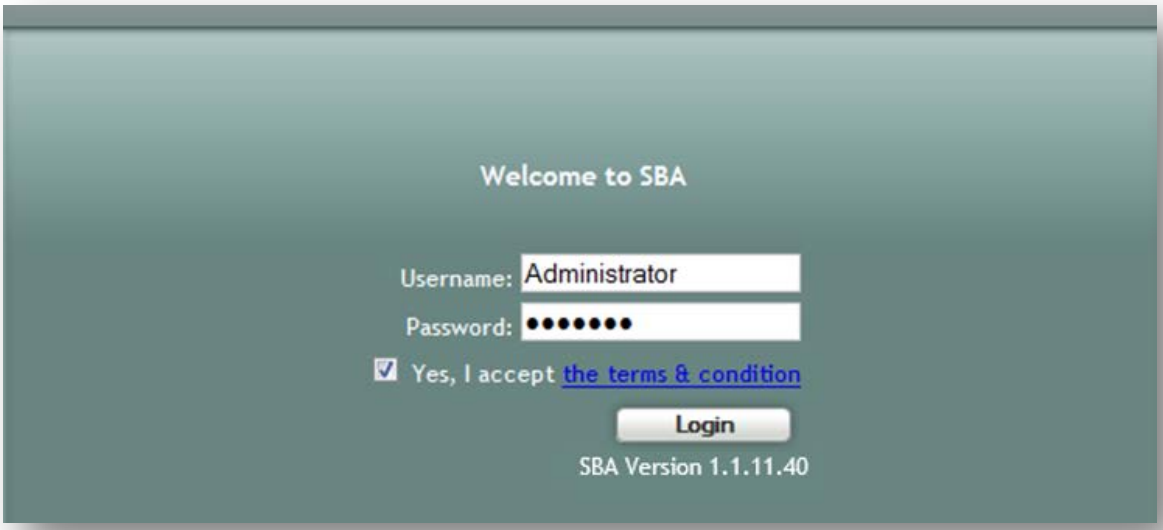


3. Open a standard Web browser (Firefox, Google Chrome, or Internet Explorer 8 and later is recommended), and then in the URL address field, enter the OSN3 server default IP address (**http://10.1.10.12**).



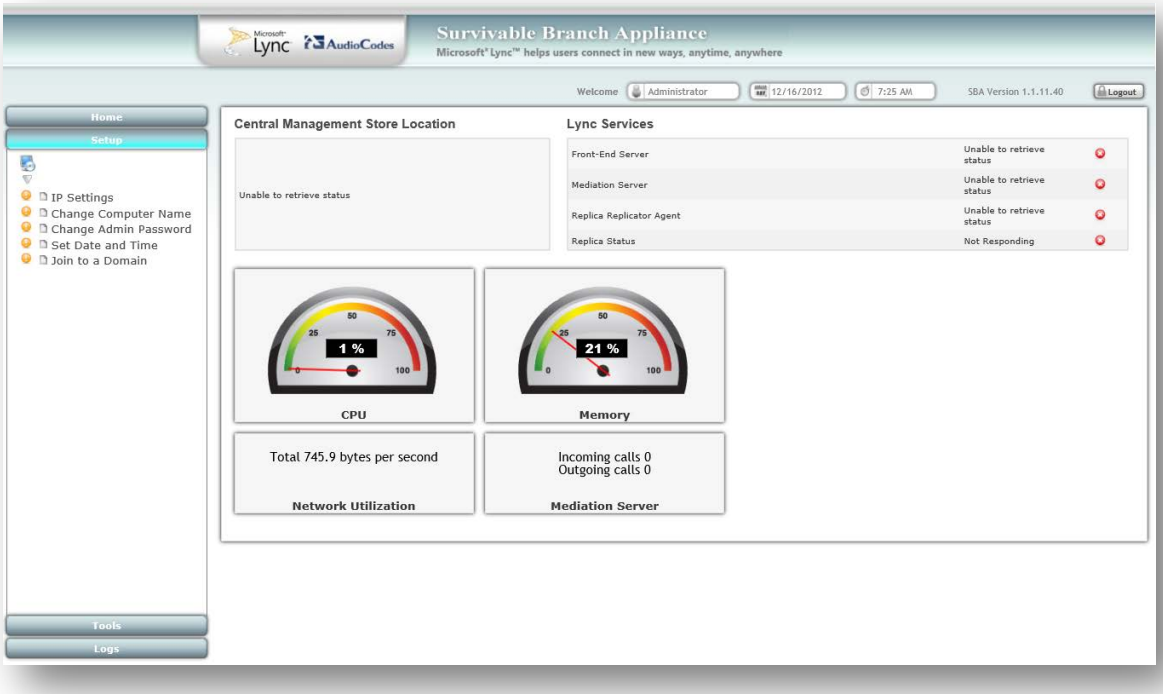
The Survivable Branch Appliance Web-based tool opens:

Figure 6-2: Welcome to SBA Screen



4. Log in with the default username ("Administrator") and password ("Pass123"), Select the "Yes, I accept the term and condition" checkbox and then click **Login**; the Home screen appears:

Figure 6-3: SBA Home Screen



Reader's Notes

7 Installing and Configuring the SBA

Once you are logged in to the SBA Web-based tool, you can start configuring SBA, as described in this section.

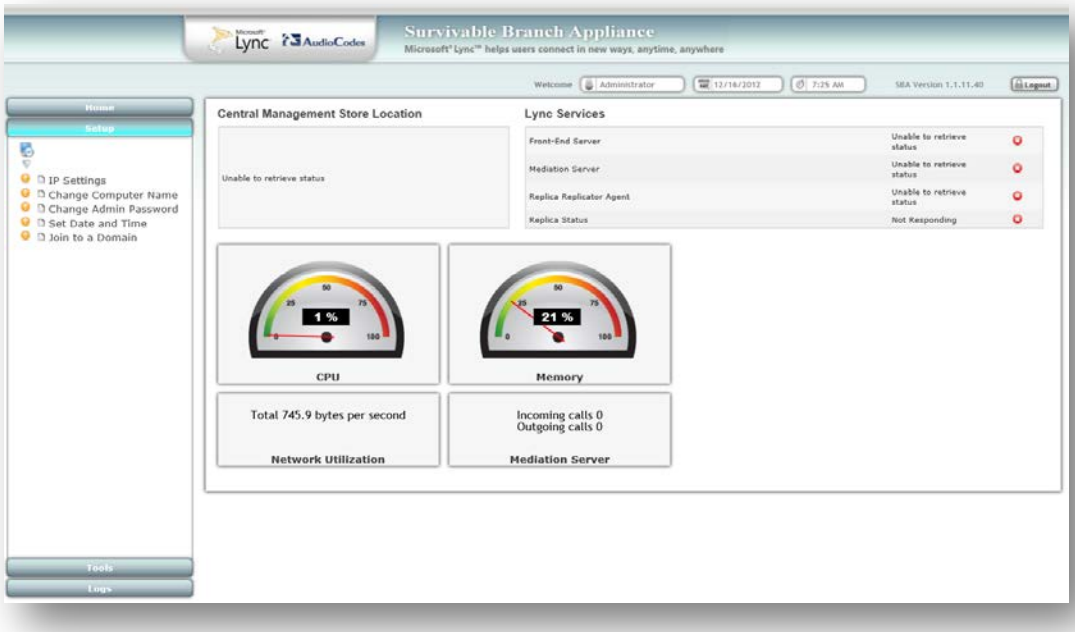
The SBA configuration is done in the **Setup** tab. For the configuration to be successful, it is imperative that all **Setup** options are performed correctly and **in sequence** (according to their order of appearance in the graphical user interface / GUI):

1. **Define IP Settings** - See Section 7.1 on page 65.
2. **Change Computer Name -** See Section 7.2 on page 70.
3. **Change Admin Password** - See Section 7.3 on page 73.
4. **Set Date and Time** - See Section 7.4 on page 75.
5. **Join to a Domain** - See Section 7.5 on page 78.
6. **Device Preparation** - See Section 7.6 on page 81.
7. **Configuration** - See Section 7.8 on page 87.
8. **Enable Replication** - See Section 7.9 on page 89.
9. **Activate Lync** - See Section 7.10 on page 91.
10. **Lync Certificate** - See Section 7.11 on page 93.
11. **Start Lync Services** - See Section 7.12 on page 99.
12. **Gateway Configuration** - See Section 7.13 on page 100.

If a task fails, ensure you correct it before continuing with additional tasks. When a task is configured successfully, a check mark (green) appears alongside the option.

Note: Initially, the **Setup** menu displays only the first few options (up till **Join to a Domain**). The remaining options appear only after you successfully define the **Joint to a Domain** option.

Figure 7-1: Setup Tab Displaying Tasks



In each of the configuration menu screens, the current CPU and memory utilization of the OSN module is displayed. In the Setup pane, a list of all the configurable items is displayed.

Table 7-1: Setup Pane Icon

Setup Pane Icon	Description
	Indicates a successfully configured item.
	Indicates an item that has not yet been configured.
	Indicates an item whose configuration has failed.

7.1 Step 1: Define IP Settings

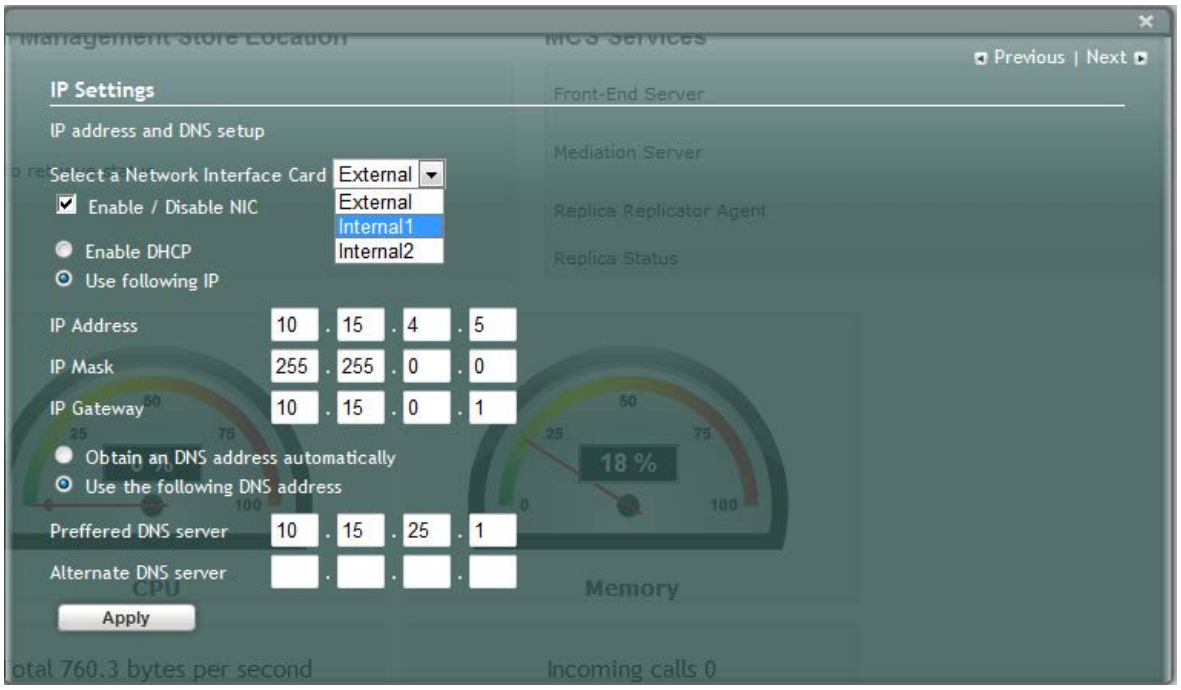
The **IP Settings** option defines the IP address and domain name server (DNS). In addition, this menu enables you to configure whether to use an internal or external NIC on the SBA device.

Note: If you previously changed the IP Settings (see Section 7.1 on page 65), skip this section.

➢ **To set the IP address and DNS:**

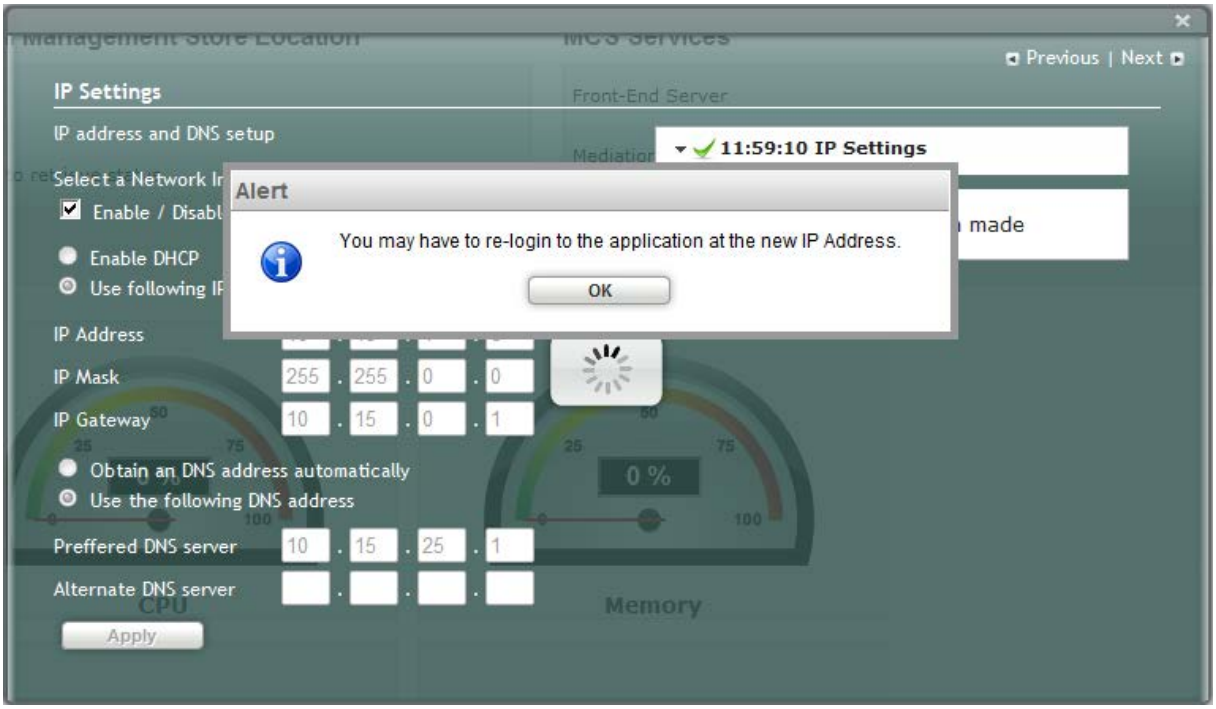
1. On the Setup menu, click **IP Settings**; the following screen appears.

Figure 7-2: Set IP Configuration Page



2. From the drop-down list, select one of the following NIC interface options:
   - **External** – The physical ports in the Mediant 1000B rear side.
   - **Internal1** – Internal port that connects to the Mediant 1000B MSBR switch. (In case using Mediant 1000B E-SBC and Gateway, this port is not connected).
   - **Internal2** – Internal port that is not connected.
3. Confirm/change the IP Address.
4. Confirm/change the IP Mask.
5. Confirm/change default IP gateway.
6. Click **Apply**. If the IP address has changed, you will be required to login again.

Figure 7-3: IP Settings – Login Again



7. Click **OK**. New login screen will appear.
8. Enter the Username, Password and click **Login**.

Notes:

- The system logs in with the new IP address.
- Every time you change the NIC interface option, click **Apply** for the change to take effect.

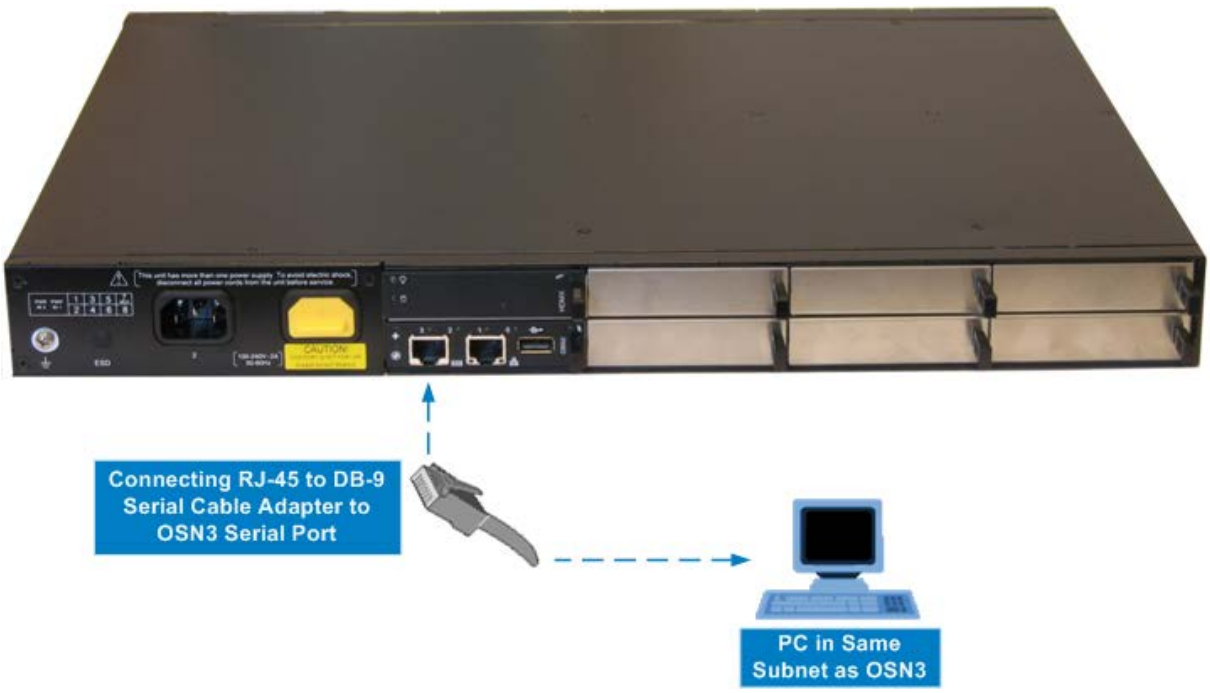
7.1.1 Using Serial Communication

You can assign an IP address to the SBA using a serial (RS-232) interface connection between a computer and the Mediant 1000B SBA OSN3 server running the SBA.

➢ **To change the IP address of the SBA using serial communication:**

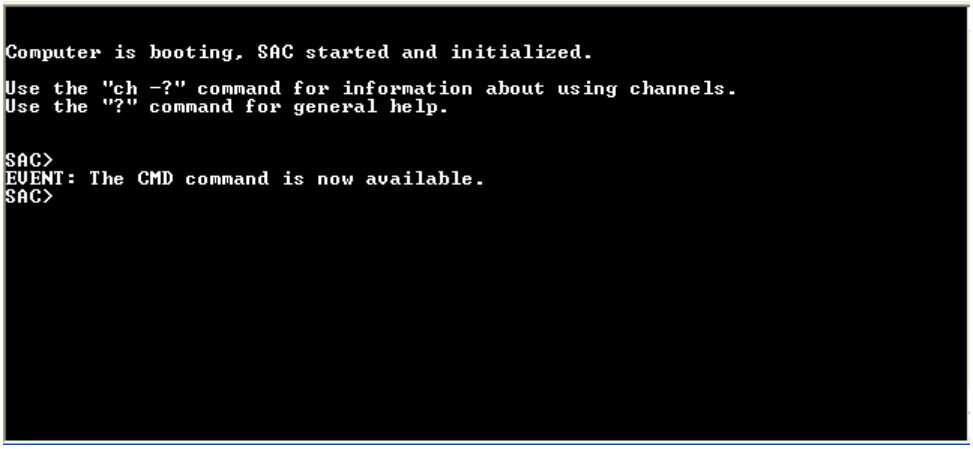
1. Connect one end of the serial cable adapter to the OSN3 serial port ( ) and the other end to the computer serial port (e.g., COM1). For information on connector pinouts, see Section 3.3.1.3 on page 26.

Figure 7-4: Serial Cabling OSN3 to Computer



2. Establish a serial communication session with the OSN3 server using a terminal emulation program such as HyperTerminal, with the following port settings:
   - **Baud Rate:** 115200 (bits per second)
   - **Data Bits:** 8
   - **Parity:** None
   - **Stop Bits:** 1
   - **Flow Control:** None

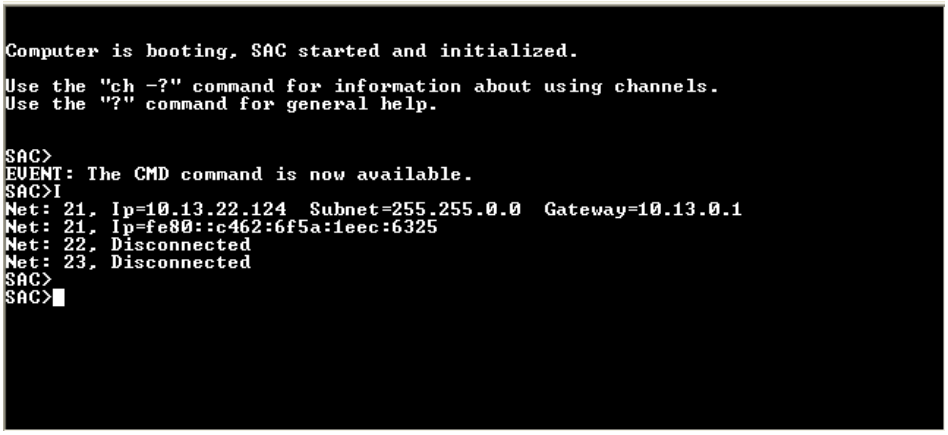
Figure 7-5: Terminal Prompt



3. At the prompt, type the following command to view all the network addresses:

```
i
```

Figure 7-6: List of Network Addresses



4. At the prompt, change the IP address of the specific Net ID to one that suits your environment, using the following command:

```
i <Net ID> <IP address> <subnet> <default gateway>
```

5. Press **Enter** to apply your settings.
6. Disconnect the serial cable from the OSN3 server.

Figure 7-7: Login Screen

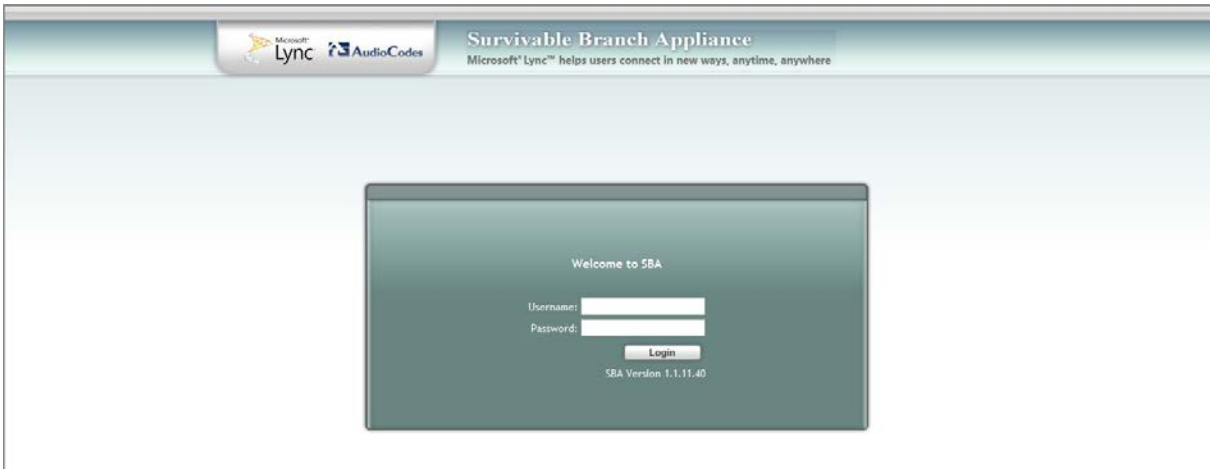
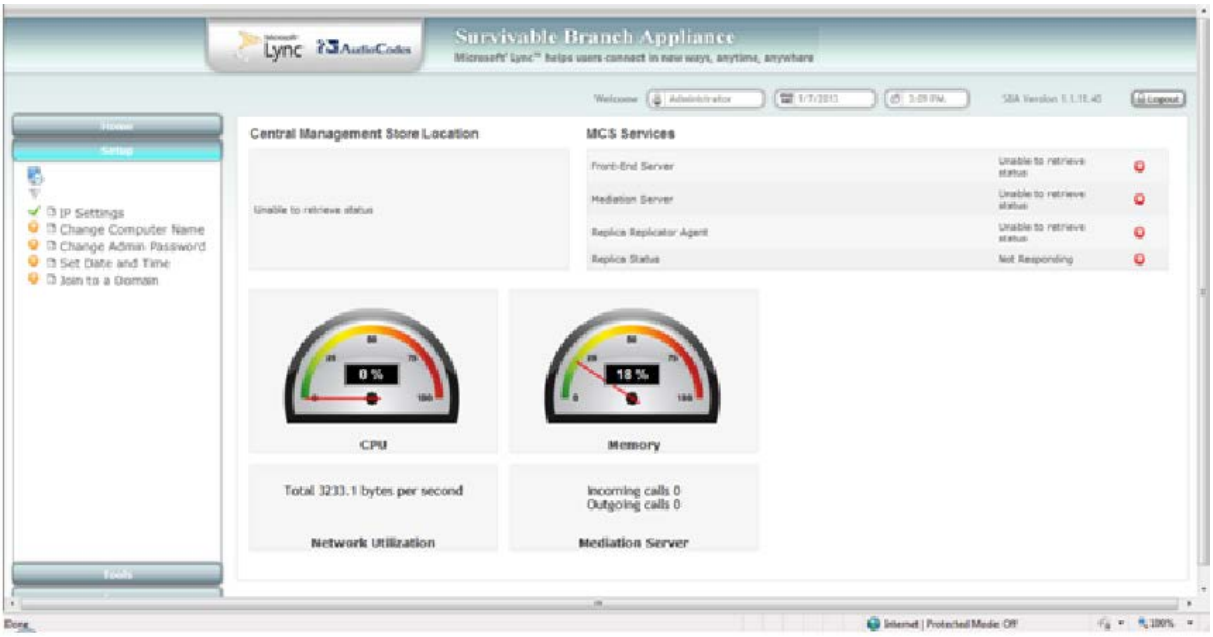


Figure 7-8: IP Settings - Complete



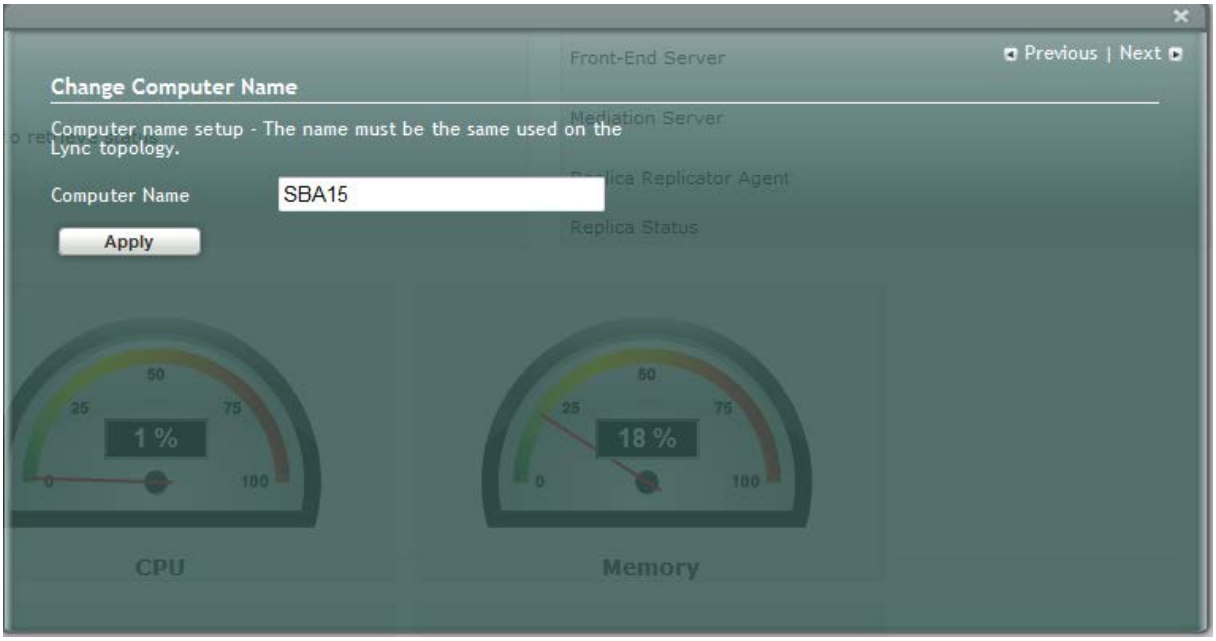
7.2 Step 2: Change Computer Name

The **Change Computer Name** option defines the computer name of the SBA.

➢ **To change the computer name:**

1. Under the **Setup** menu tab, click the **Change Computer Name** option; the following screen appears:

Figure 7-9: Change Computer Name Screen

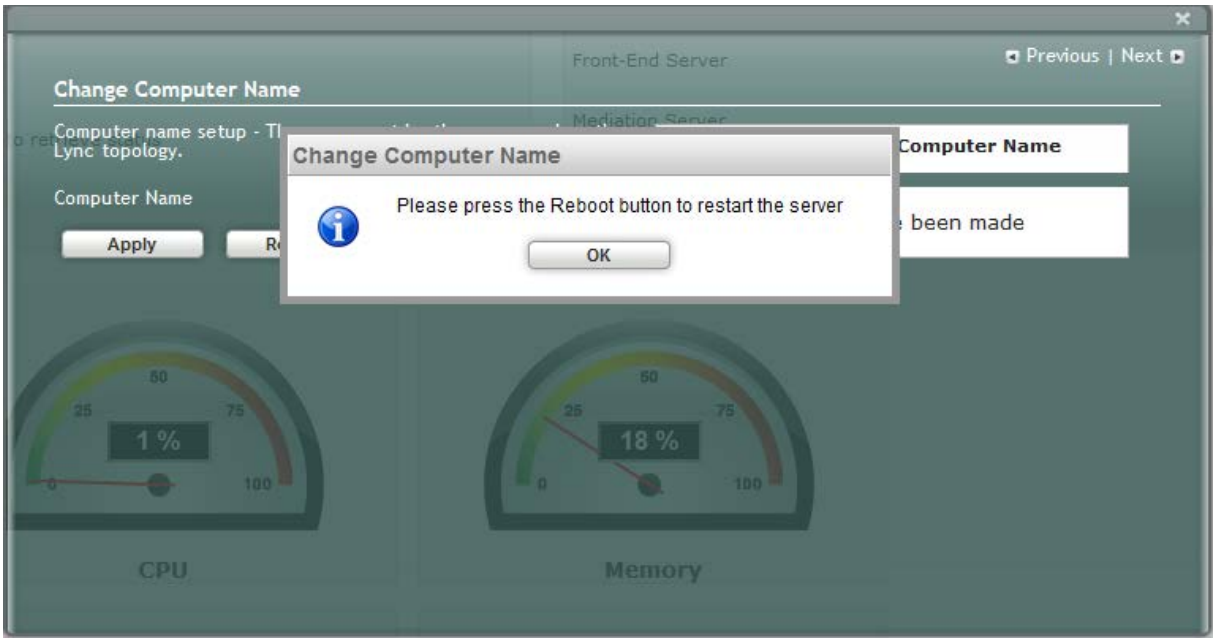


2. In the **Computer Name** field, enter the computer name.

Note: The Computer Name must be the same as that used for the SBA in the Microsoft Active Directory (AD) and Topology during the pre-configuration steps done at the datacenter (see Section 5 on page 47).

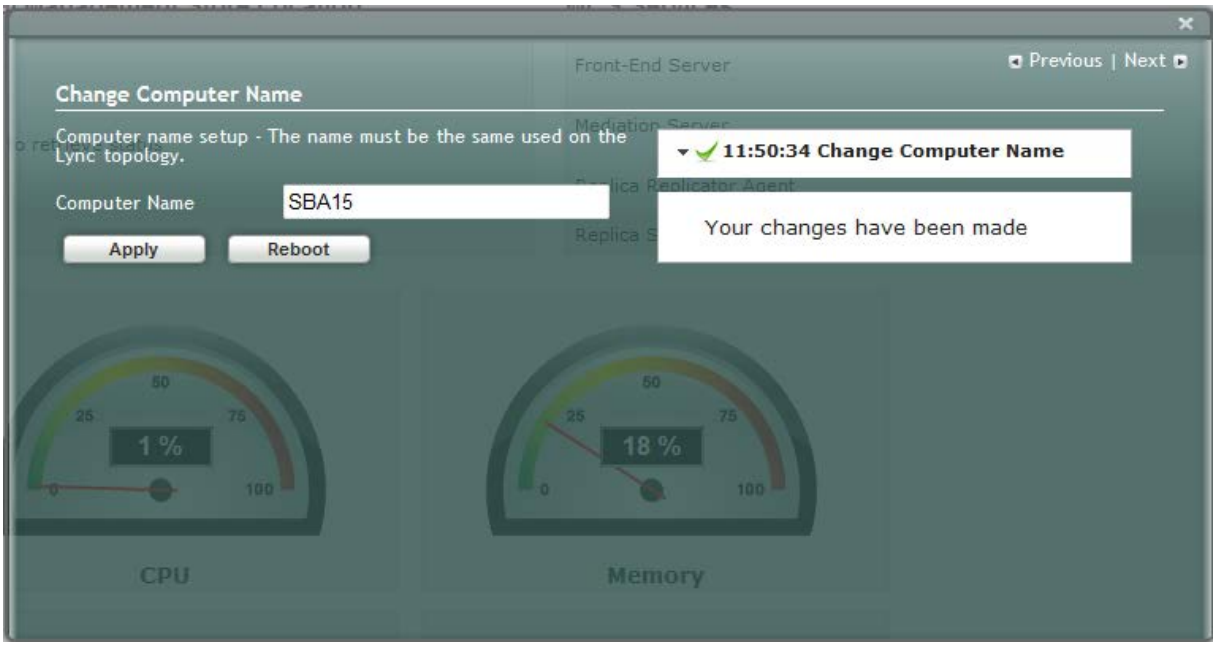
3. Click **Apply**; the "Operation Completed Successfully" message appears on the bottom of the screen. A message also appears to advise that a re-boot is necessary for the setting to take effect:

Figure 7-10: Change Computer Name - Reboot



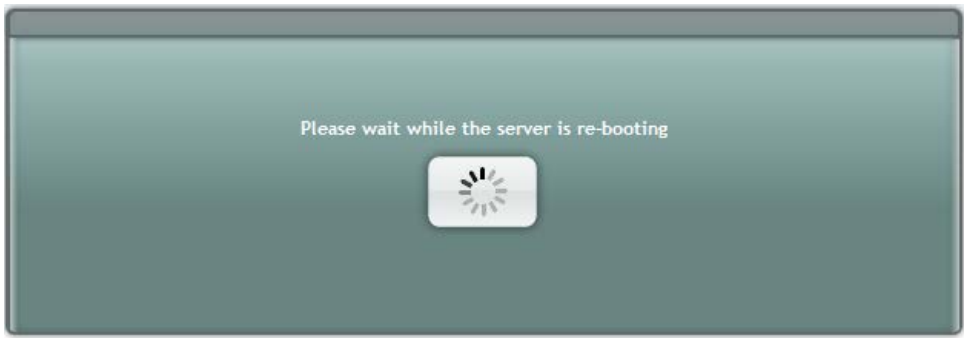
4. Click **OK**; the following screen appears.

Figure 7-11: Change Computer Name – Applied Changes



5. Click **Reboot**; the SBA reboots and the following screen is displayed:

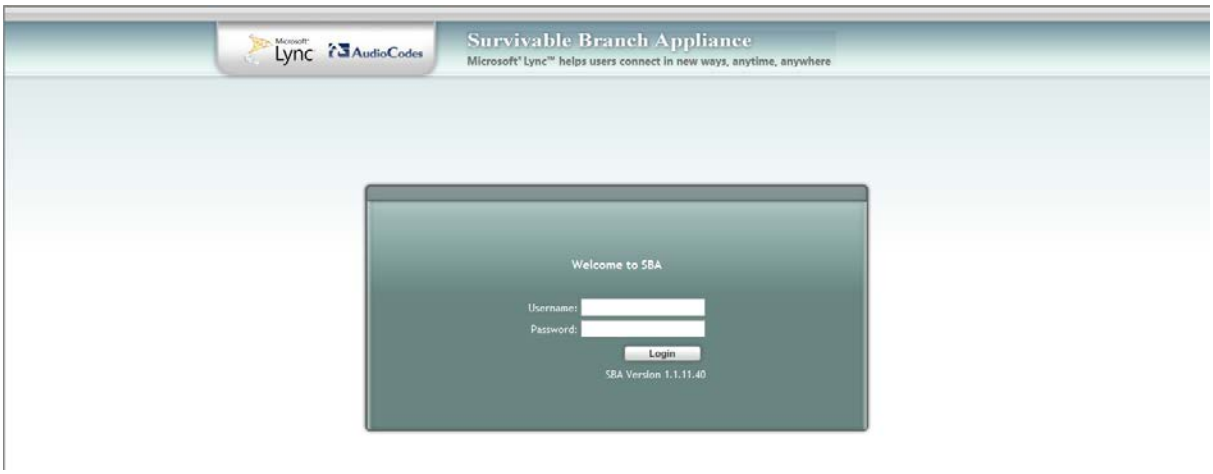
Figure 7-12: Server Re-booting



Note: The re-boot process takes approximately five minutes.

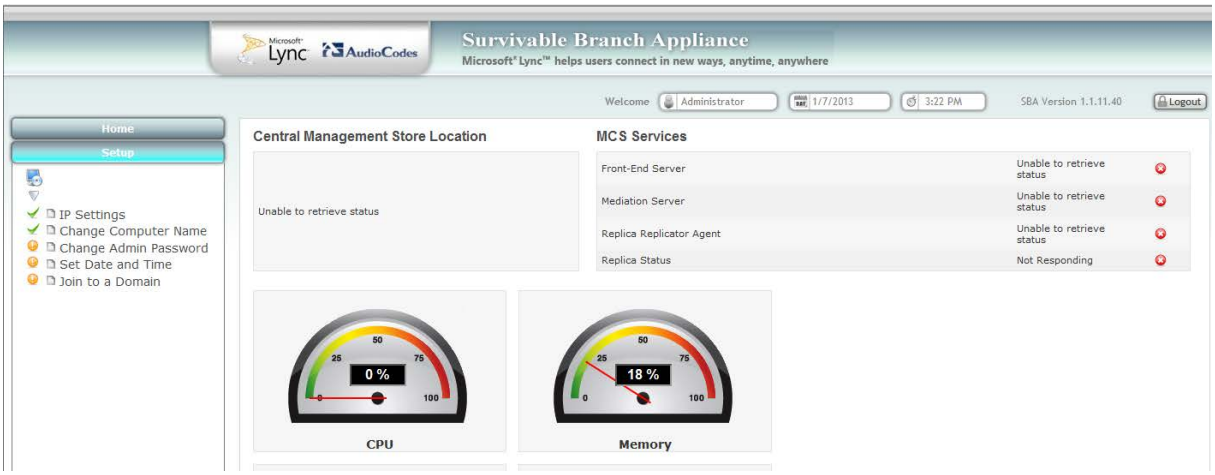
When the SBA completes its reboot, the Welcome to SBA screen appears again.

Figure 7-13: Login Screen



6. Enter your username and password and then click **Login** to log in once again to the SBA Web-based tool; the **Setup** menu tab appears, displaying a green check mark alongside the **Change Computer Name** option, as shown below:

Figure 7-14: Change Computer Name – Completed Successfully



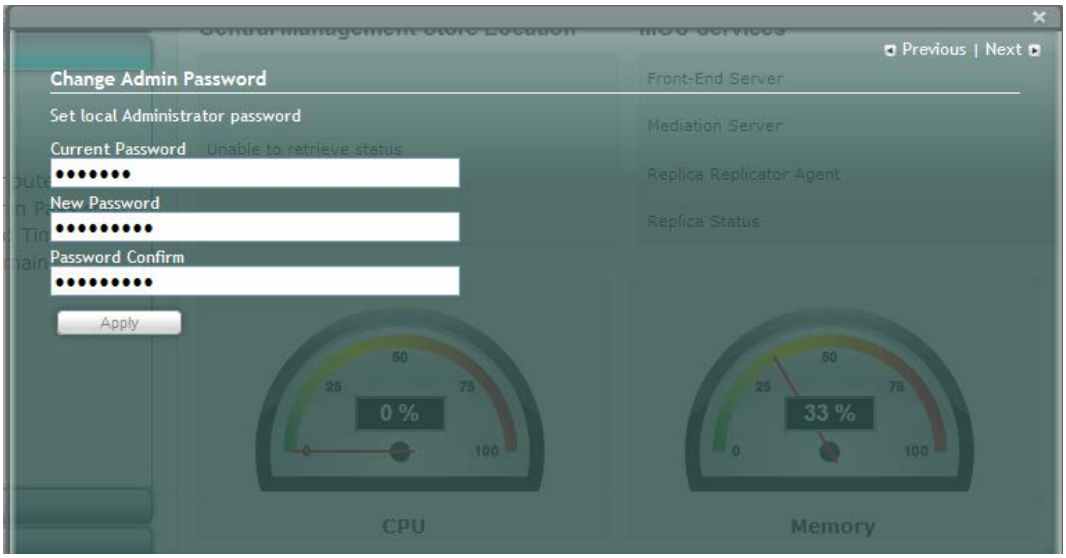
7.3 Step 3: Change Admin Password

The **Change Admin Password** option resets the local Administrator password.

➢ **To change the Administrator password:**

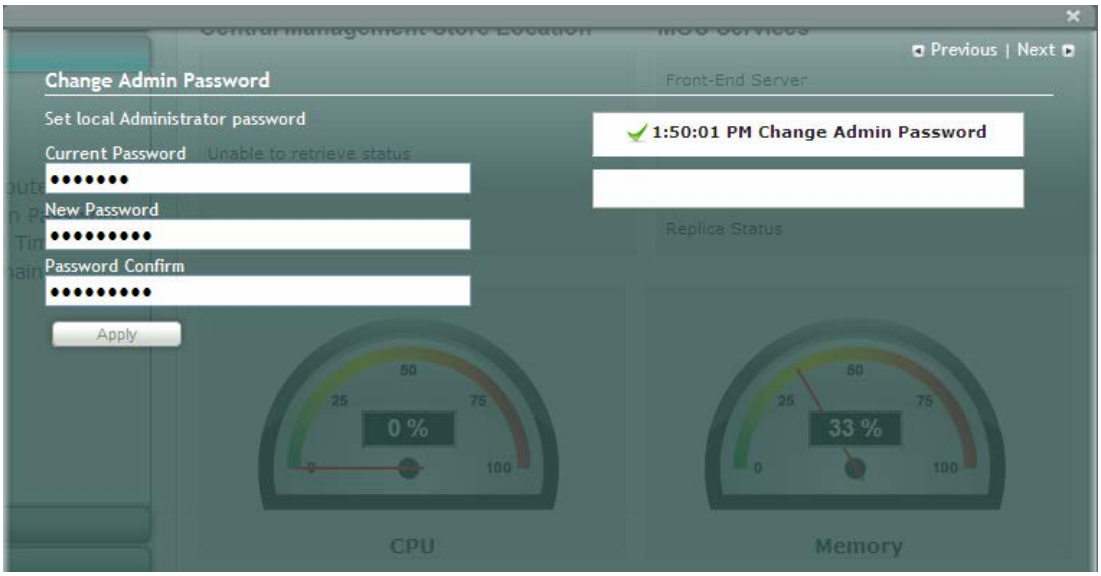
1. Under the **Setup** menu tab, click the **Change Admin Password** option; the following screen appears:

Figure 7-15: Change Admin Password Screen



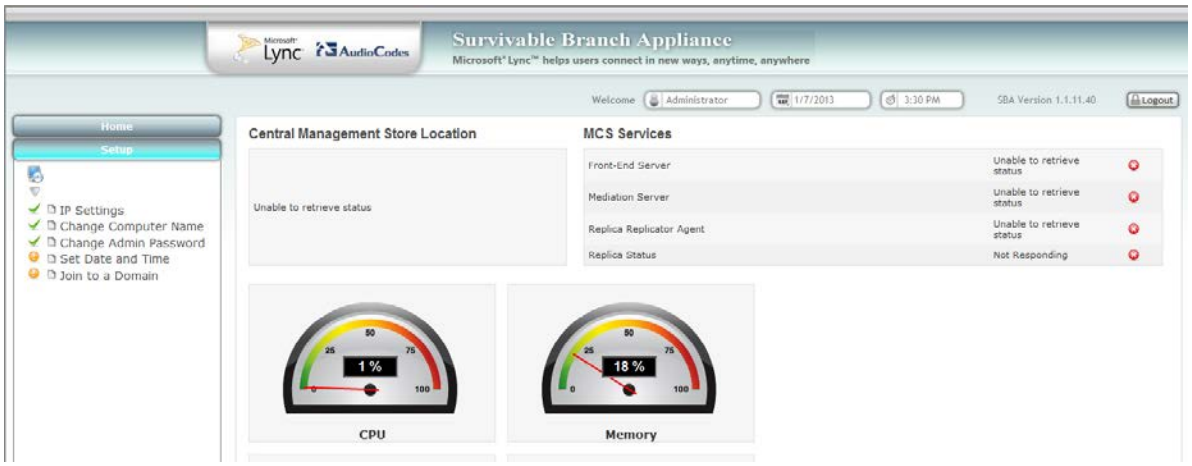
2. In the 'Current Password' field, enter the current password.
3. In the 'New Password' field', enter a new password, and then in the 'Password Confirm' field, enter the new password again.
4. Click **Apply**; the following screen appears:

Figure 7-16: Change Admin Password – Applied Changes



5. Click **Next** to proceed to the next setup task; a green check mark appears alongside the **Change Admin Password** option under the **Setup** menu tab, as shown below:

Figure 7-17: Change Admin Password – Completed Successfully



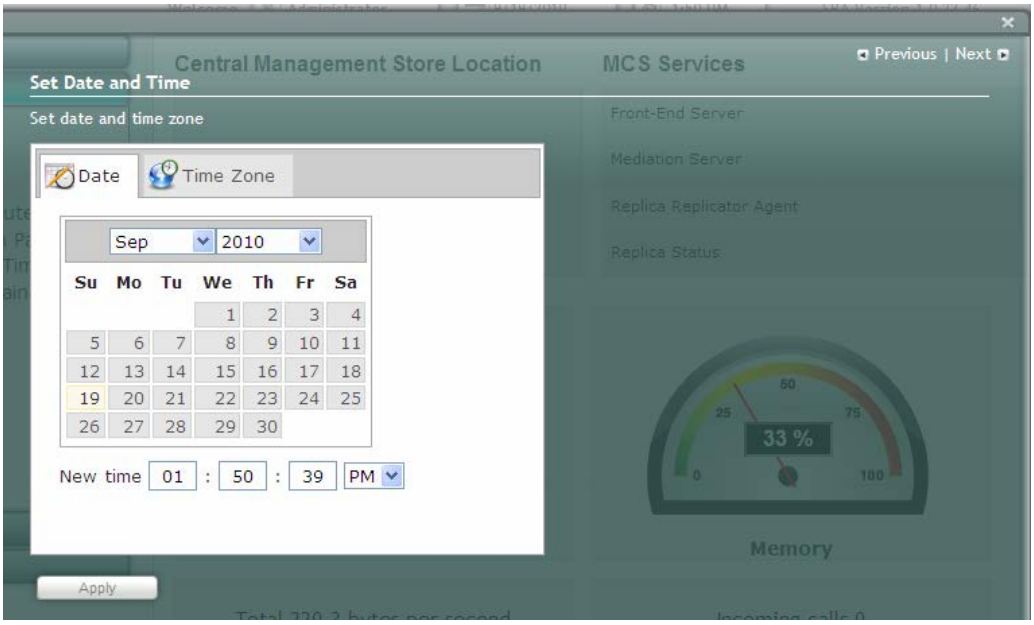
7.4 Step 4: Set Date and Time

The **Set Date and Time** option resets the date and time zone.

➢ **To set the date and time:**

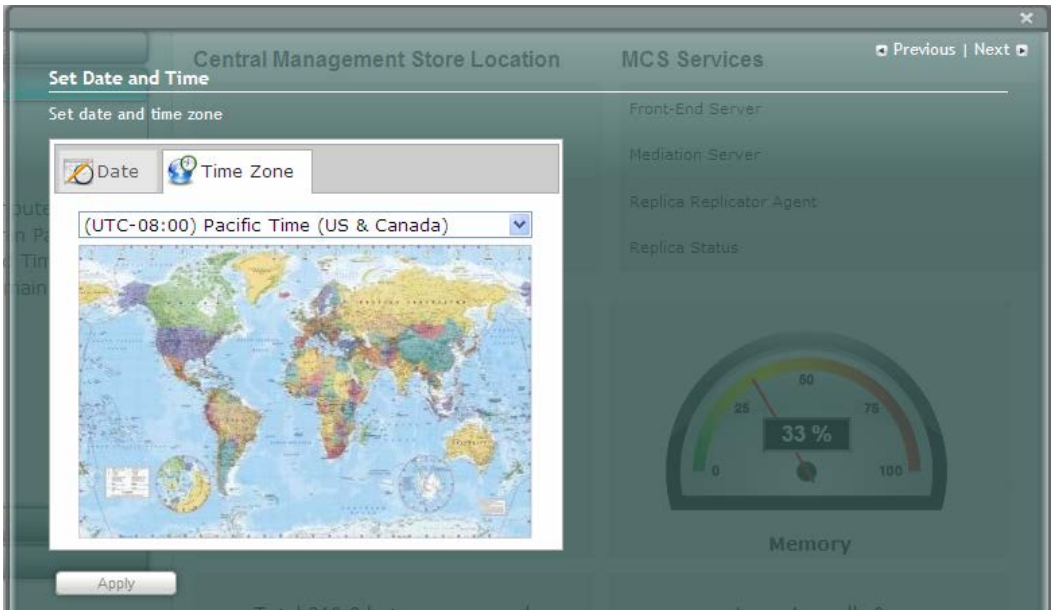
1. Under the **Setup** menu tab, select the **Set Date and Time** option; the following screen appears:

Figure 7-18: Set Date and Time Screen



2. Select the **Time Zone** tab; the following screen appears:

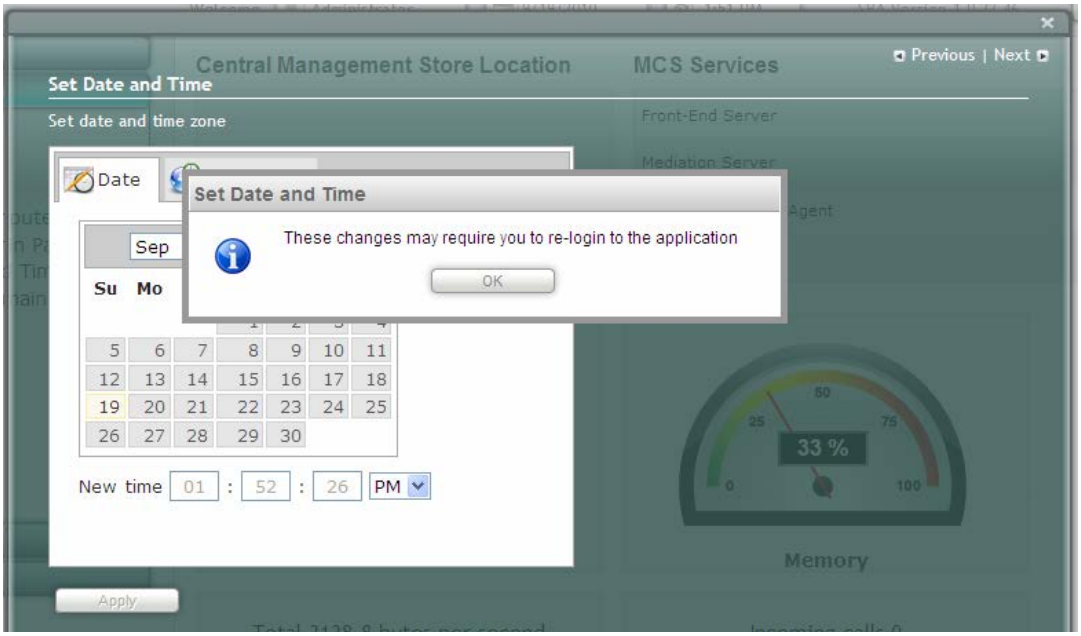
Figure 7-19: Set Date and Time - Time Zone



3. From the drop-down list, select the appropriate time zone.
4. Select the **Date** tab, and then define the date and time.
5. Click **Apply**; the “Operation Completed Successfully” message appears on the bottom of the screen.

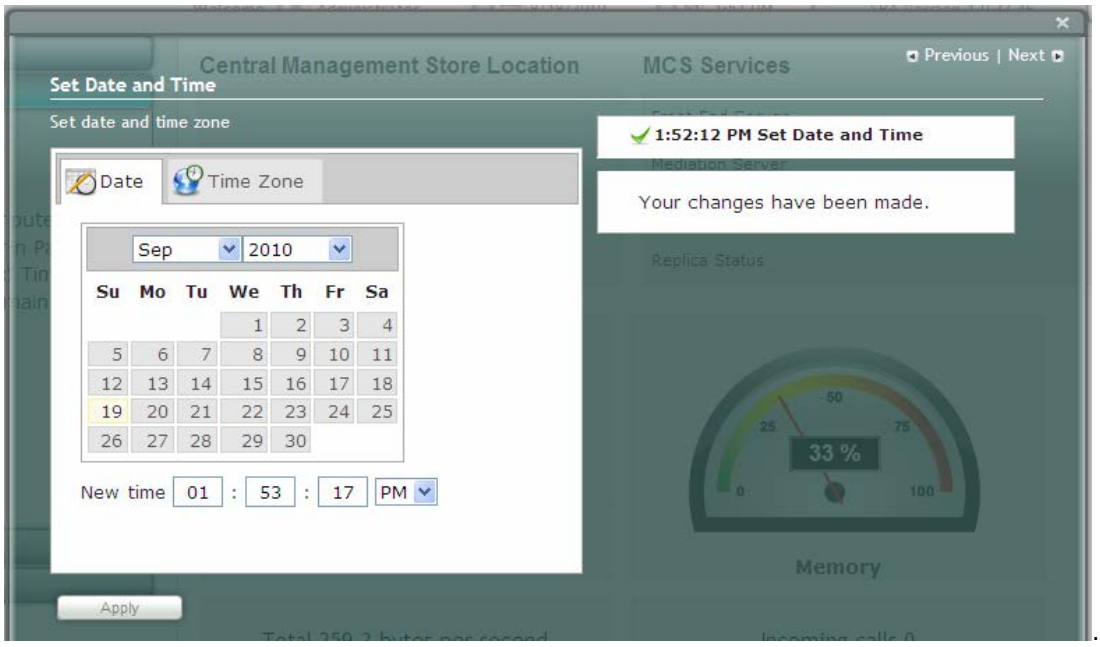
6. Click **Apply;** a notification message box appears:

Figure 7-20: Set Date and Time – Notification Message



7. Click **OK**; the following confirmation screen appears:

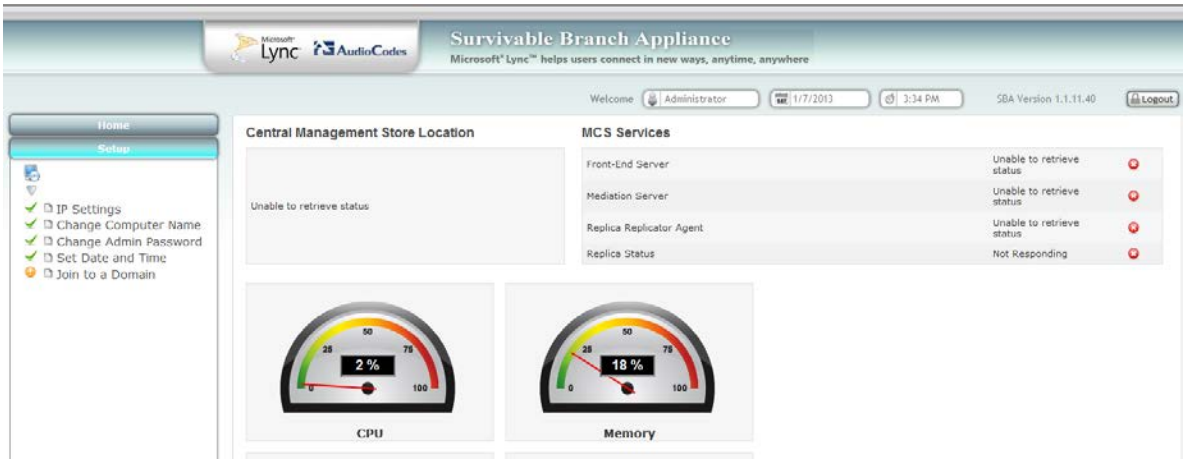
Figure 7-21: Set Date and Time – Applied Changes



8. Click **Next** to proceed to the next setup task.

A green check mark appears alongside the **Set Date and Time** option under the **Setup** menu tab, as shown below:

Figure 7-22: Set Date and Time - Completed Successfully



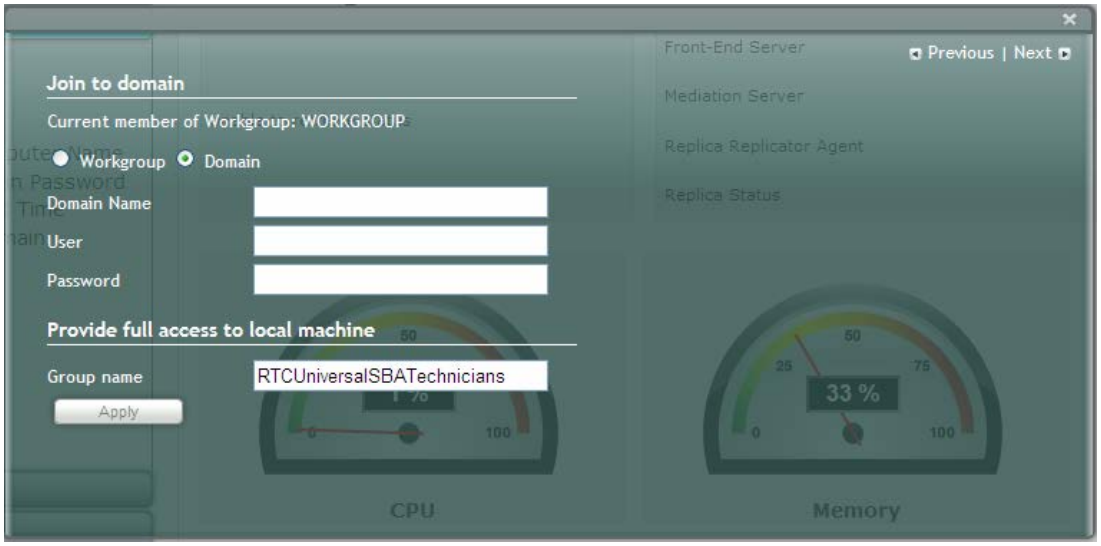
7.5 Step 5: Join to a Domain

The **Join to Domain** option enables you to join the SBA application to a domain.

➢ **To join the SBA application to a domain:**

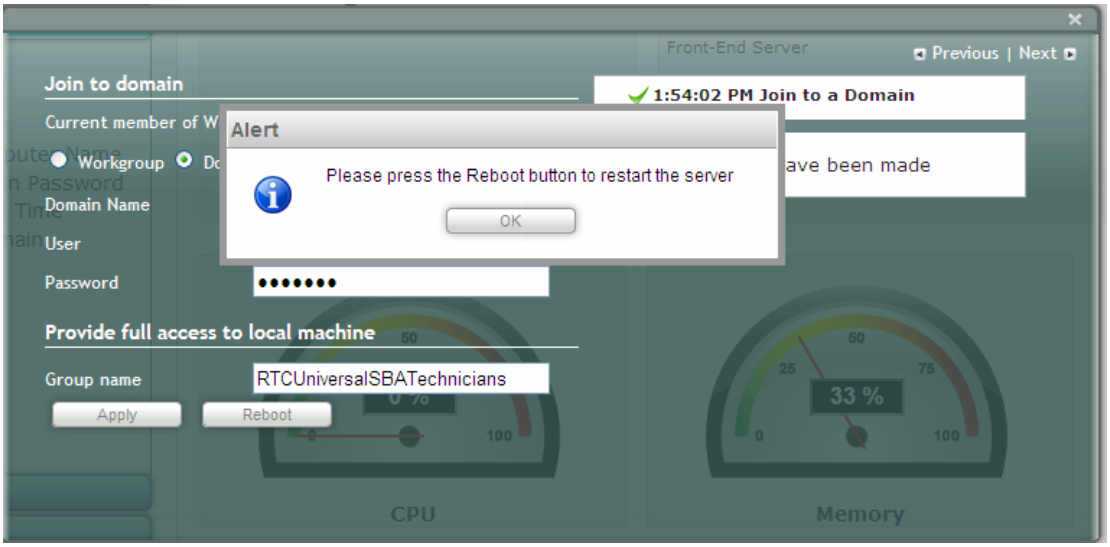
1. Under the **Setup** menu, click the **Join to a Domain** option; the following screen appears:

Figure 7-23: Join to a Domain Screen



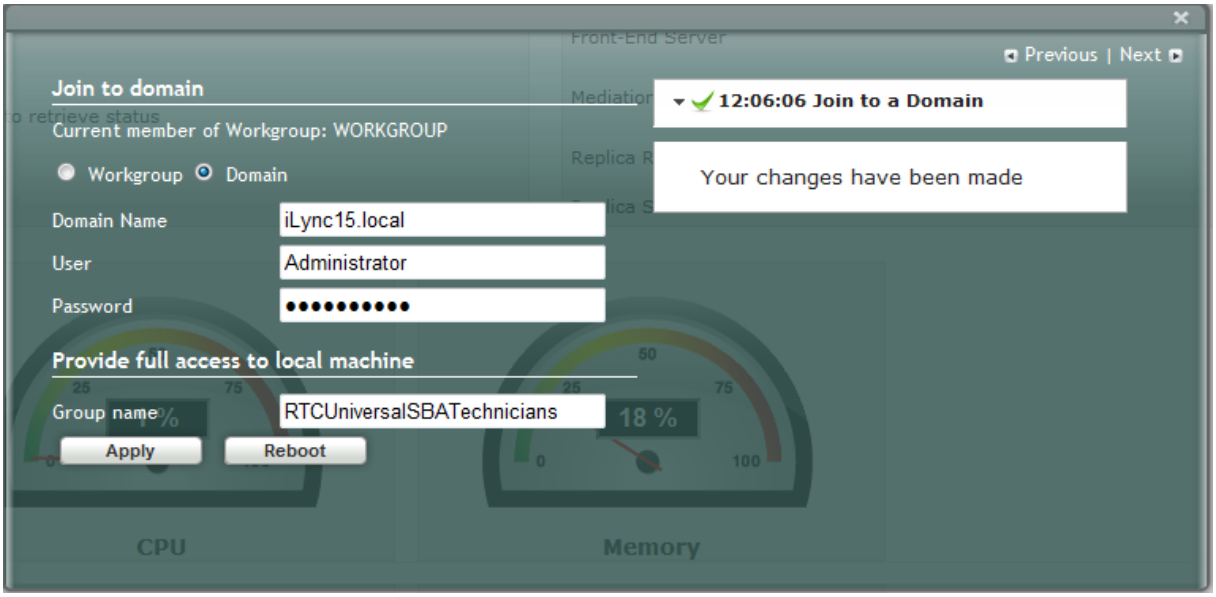
2. In the 'Domain Name' field, enter the domain name.
3. In the 'User' and 'Password' fields, enter the user and password of an account that has permission to join the SBA to the domain as configured in Section 5.1 on page 47.
4. In the 'Group name' field, ensure that the **RTCUniversalSBATechnicians** value is selected.
5. Click **Apply**; a message box appears requesting you to confirm reboot:

Figure 7-24: Join to a Domain – Reboot Message Box



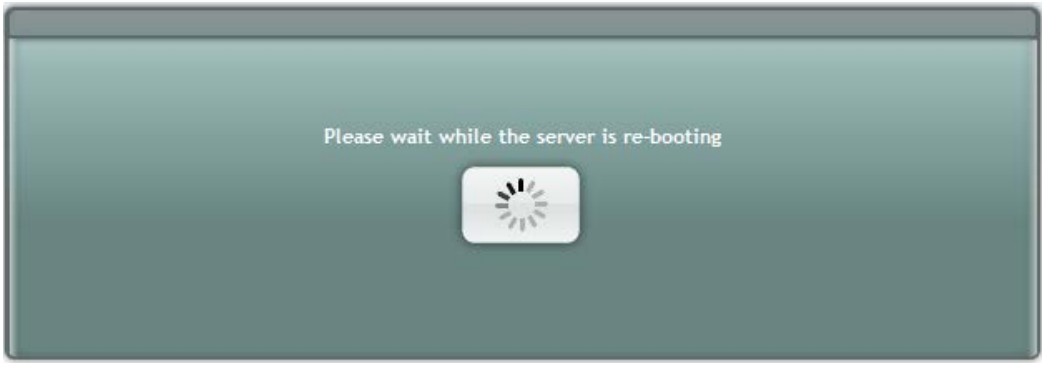
6. Click **OK**; the following screen appears:

Figure 7-25: Join to a Domain – Applied Changes



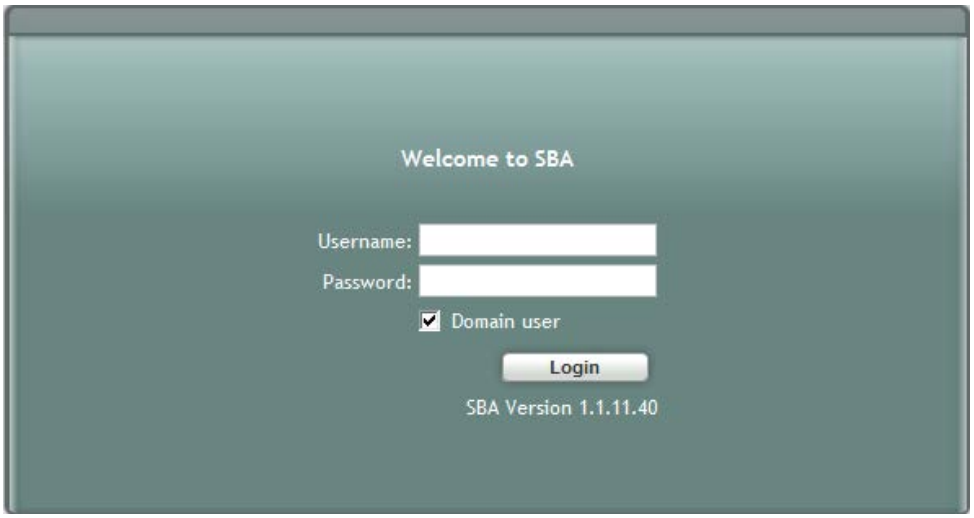
7. Click **Reboot** to reboot the OSN server; the following screen appears:

Figure 7-26: Server Rebooting



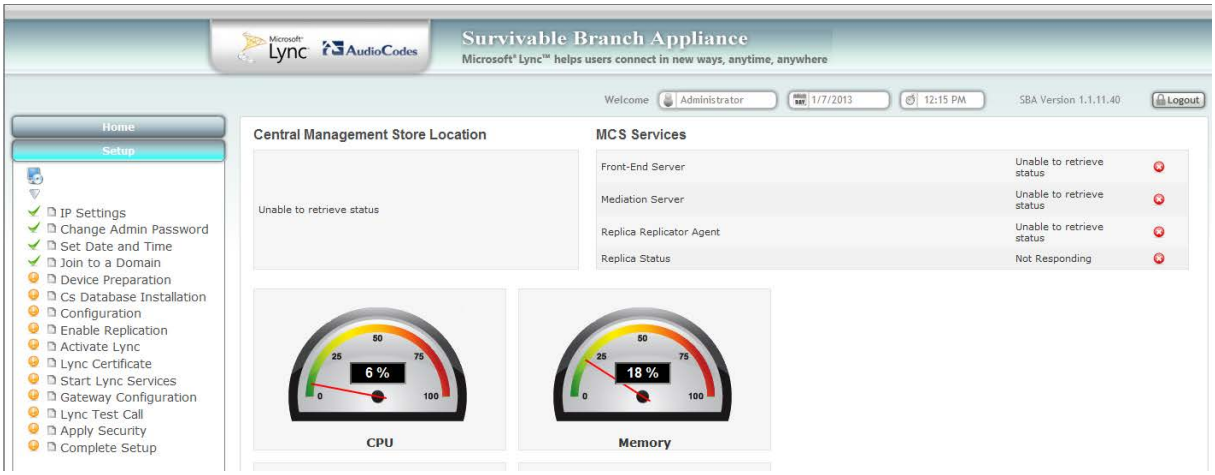
8. When the reboot completes, the Welcome to SBA login screen appears, now displaying a **Domain user** check box (which is selected by default):

Figure 7-27: Welcome to SBA



9. Log in with the Domain user username and password, and then click **Login**; a green check mark is displayed alongside the **Join to a Domain** option under the **Setup** menu tab, as shown below. In addition, the **Setup** menu now displays the remaining menu options.

Figure 7-28: Join to a Domain - Completed Successfully



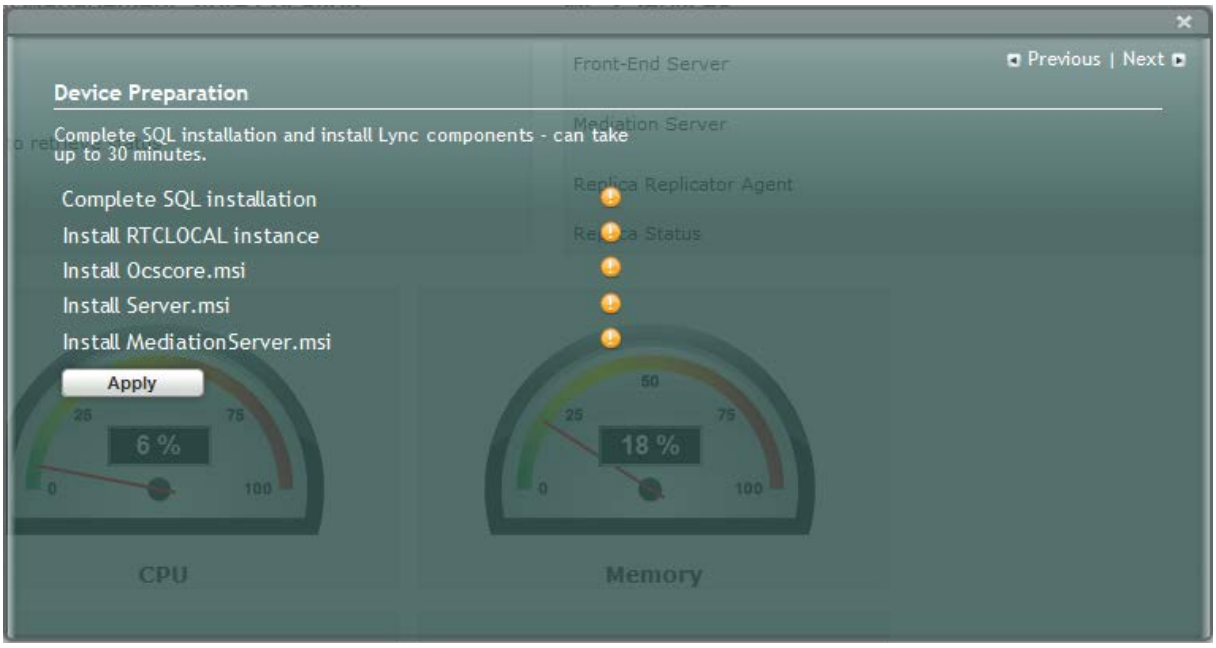
7.6 Step 6: Device Preparation

The **Device Preparation** menu option completes the SQL preparation and installs the Lync Server 2013 components.

➢ **To prepare the device:**

1. Under the **Setup** menu, click the **Device Preparation** option; the following screen appears:

Figure 7-29: Device Preparation Screen



2. Click **Apply**; the SQL installation begins, and the following screens appear in sequence as the SQL installation progresses. You can view a detailed log after each installation phase, by clicking the **Detailed Log** link.

Figure 7-30: Device Preparation - Started

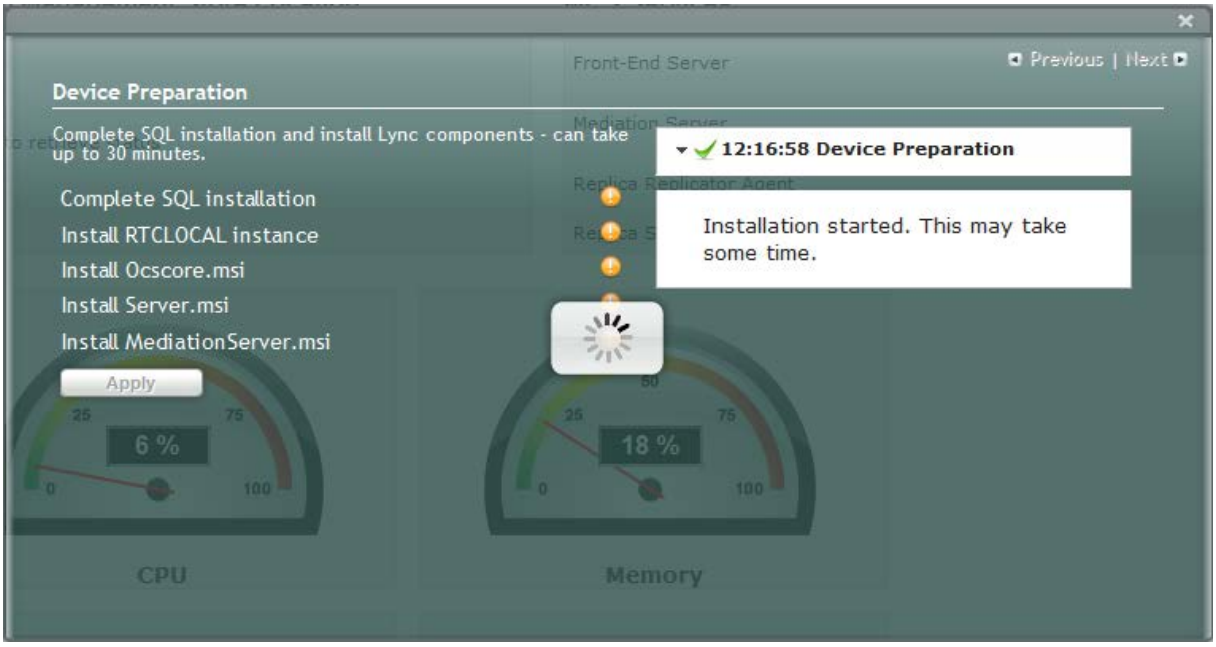


Figure 7-31: Device Preparation – SQL Installation

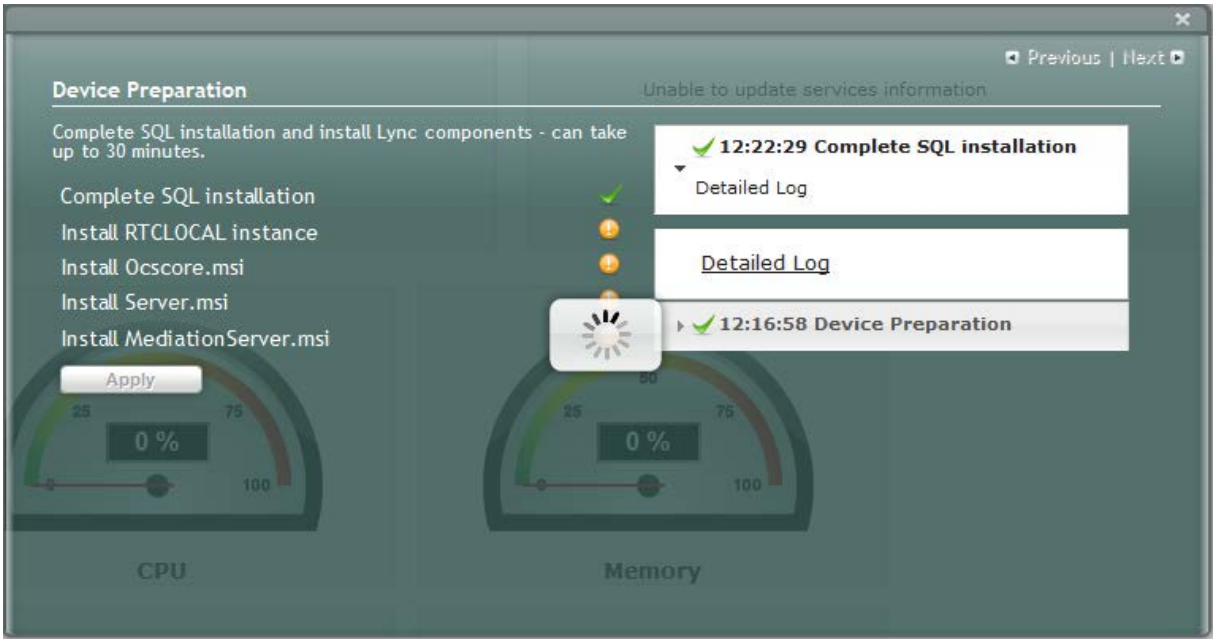


Figure 7-32: Device Preparation – Install RTCLOCAL instance

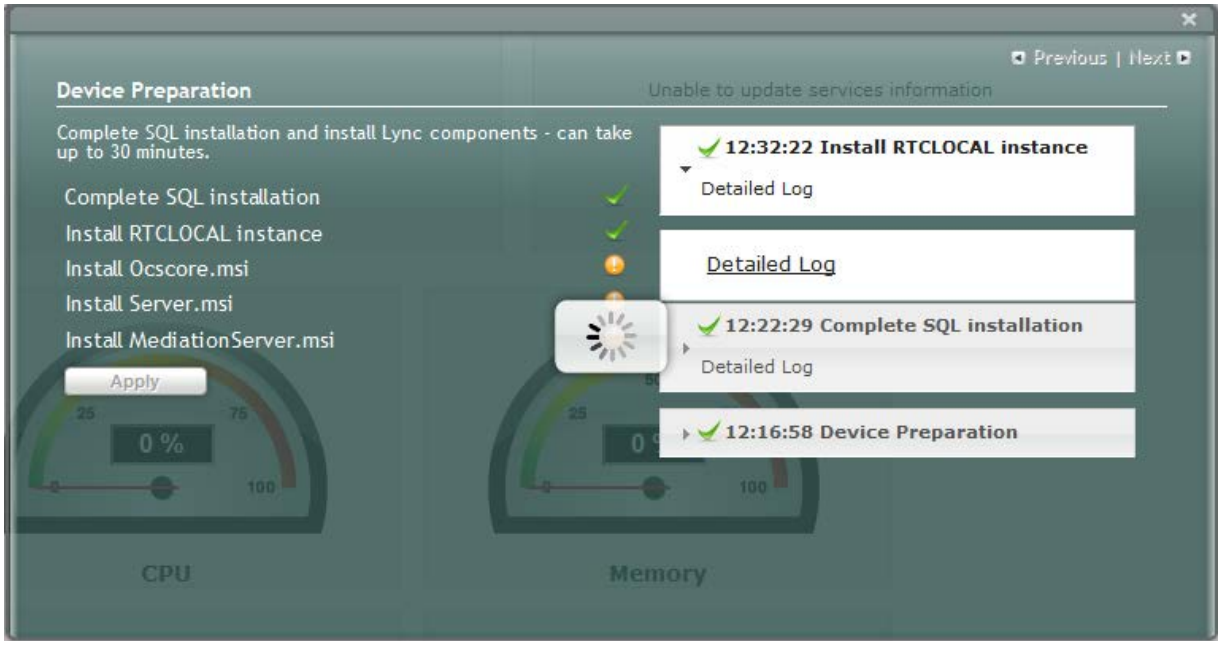


Figure 7-33: Device Preparation – Ocscore Installation

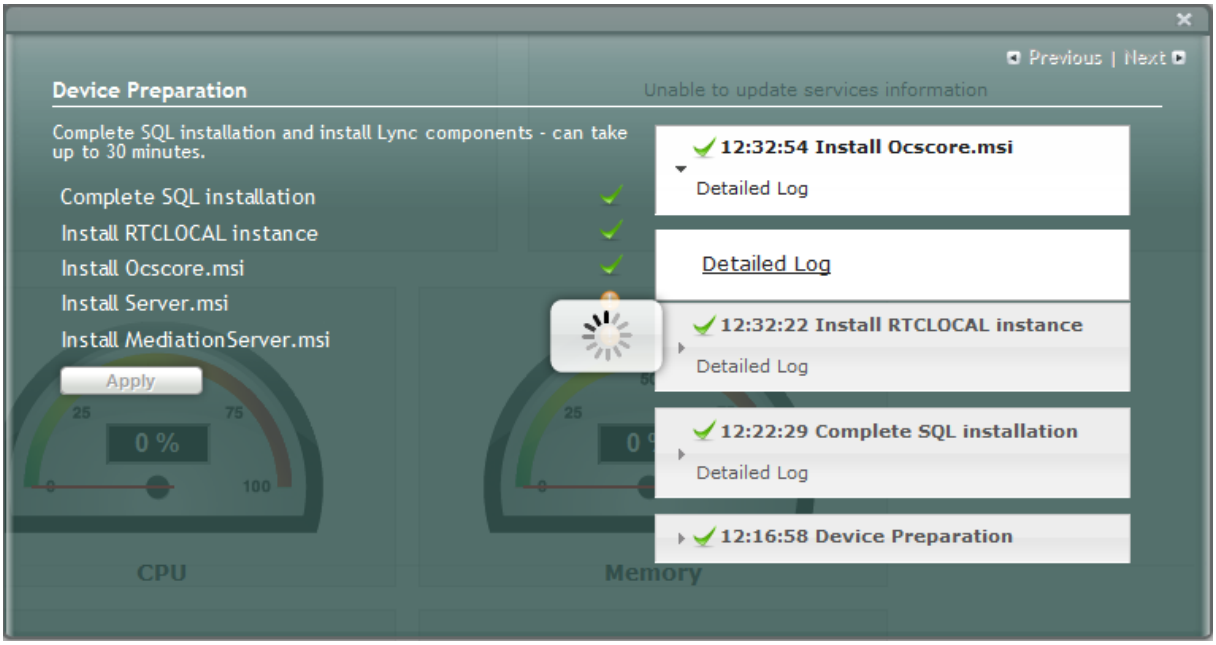


Figure 7-34: Device Preparation – Server Installation

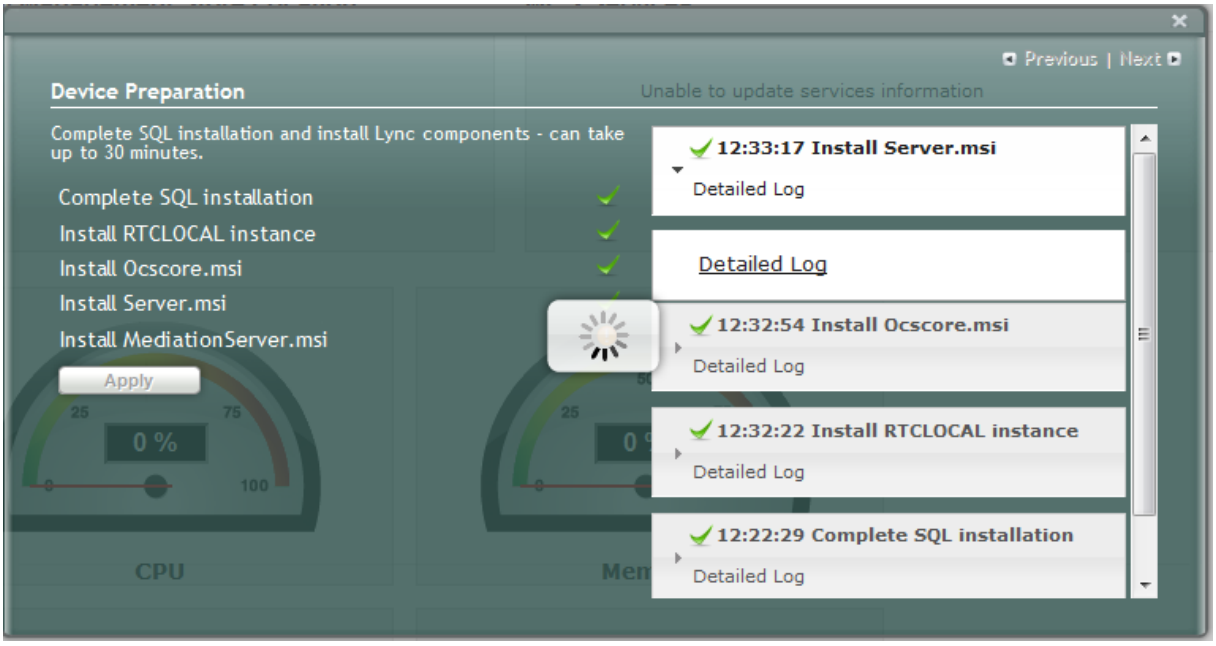
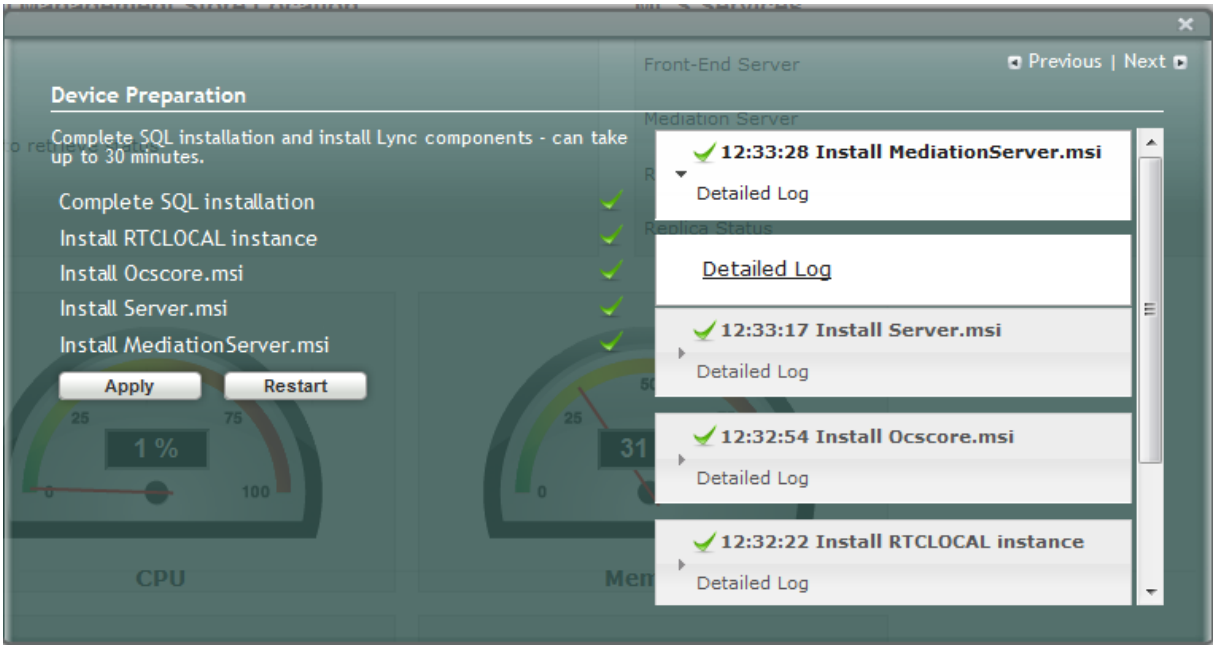
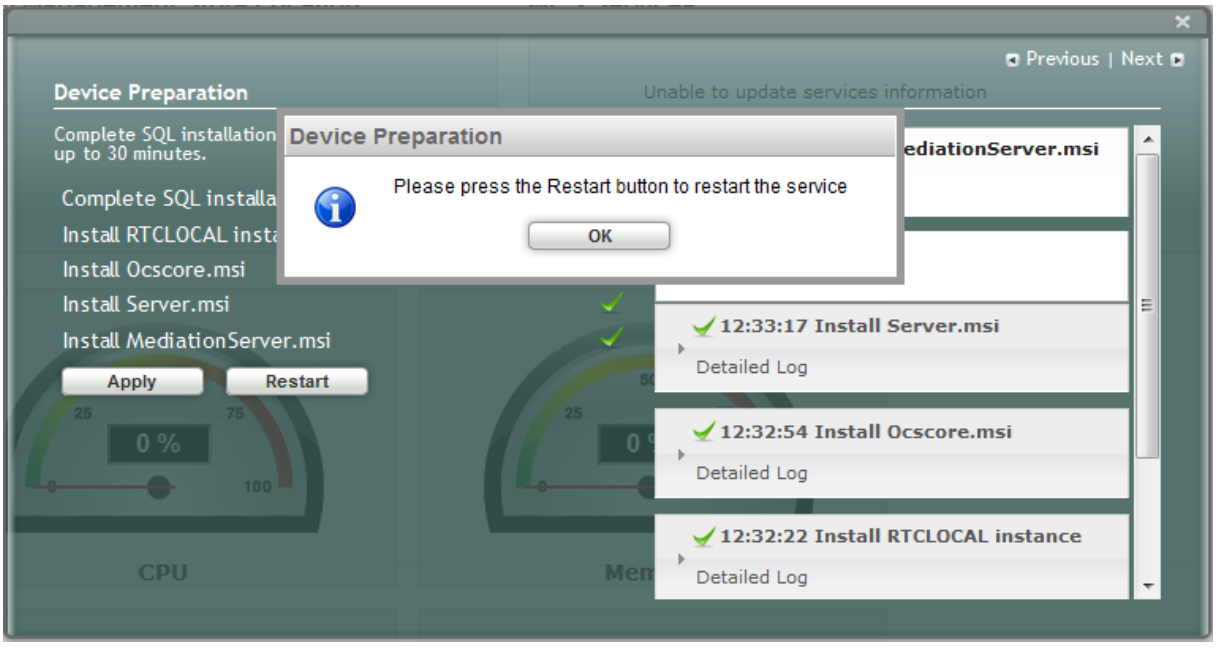


Figure 7-35: Device Preparation – Mediation Server Installation



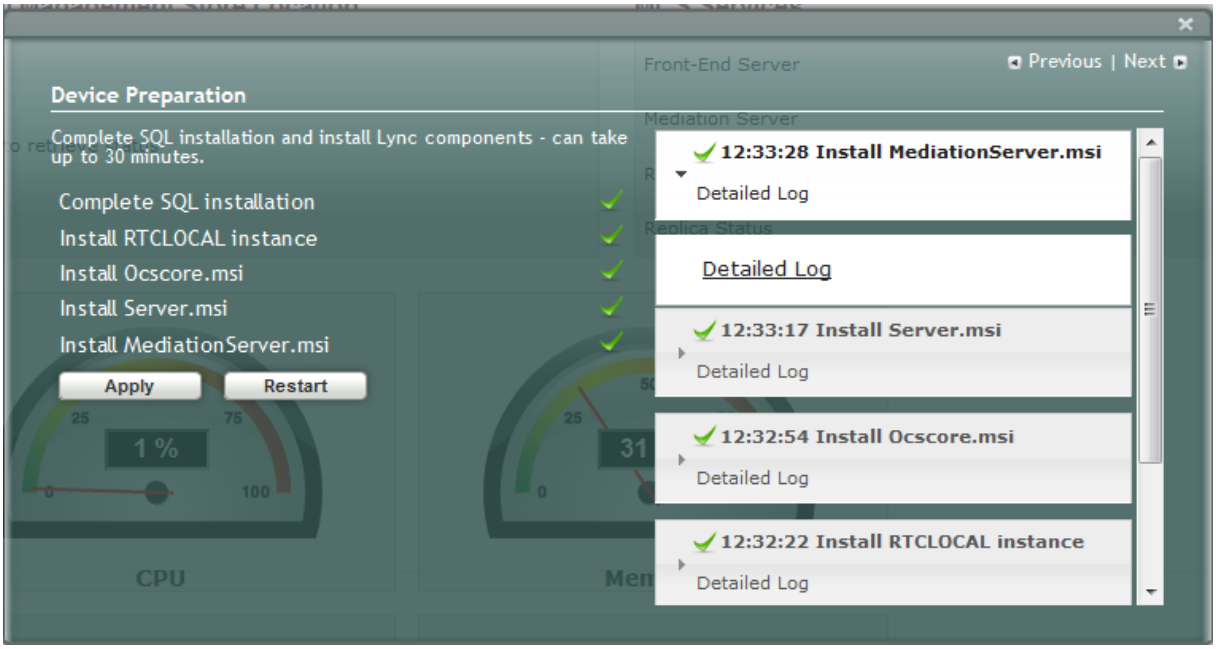
When installation completes, you are notified to click the **Restart** button to restart the server services:

Figure 7-36: Device Preparation – Restart Message Box



3. Click **OK**; the following screen appears:

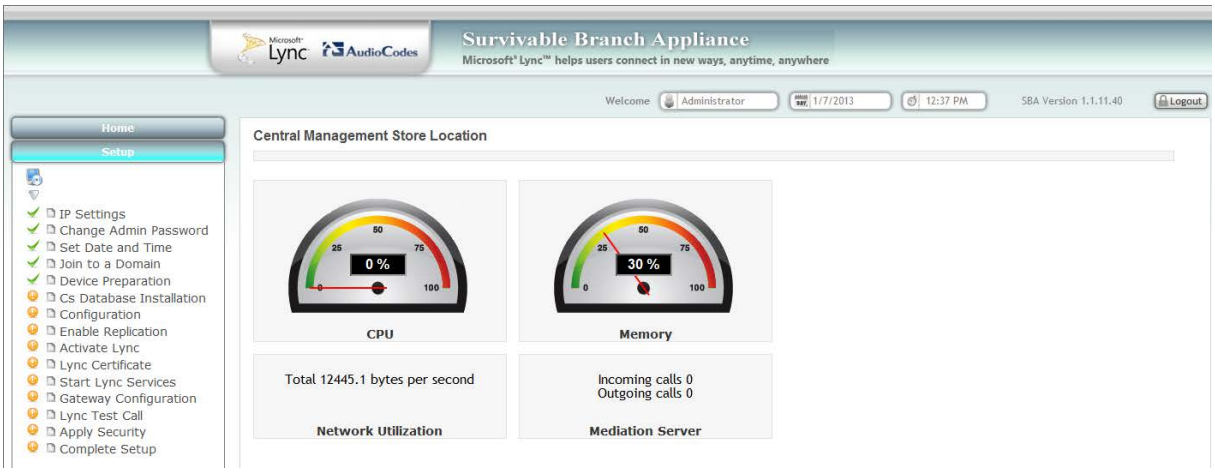
Figure 7-37: Device Preparation – Restart



4. If all steps have been completed successfully, click **Restart**. If not, refer to the Detailed Log for corrective information, rectify the problem, and then click **Apply** to install the remaining components.

   A green check mark appears alongside the **Device Preparation** option under the Setup menu, as shown below:

Figure 7-38: Device Preparation – Completed Successfully



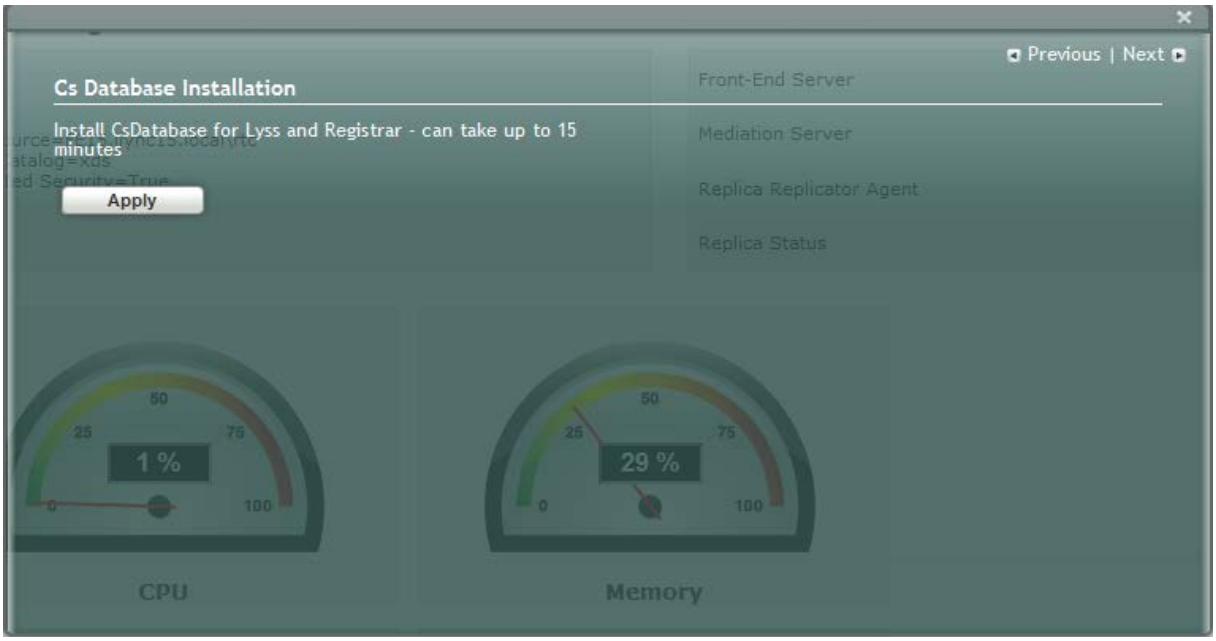
7.7 Step 7: Cs Database Installation

The **CS Database installation** option installs CsDatabase for Lyss and registrar

➢ **To install the CsDatabase:**

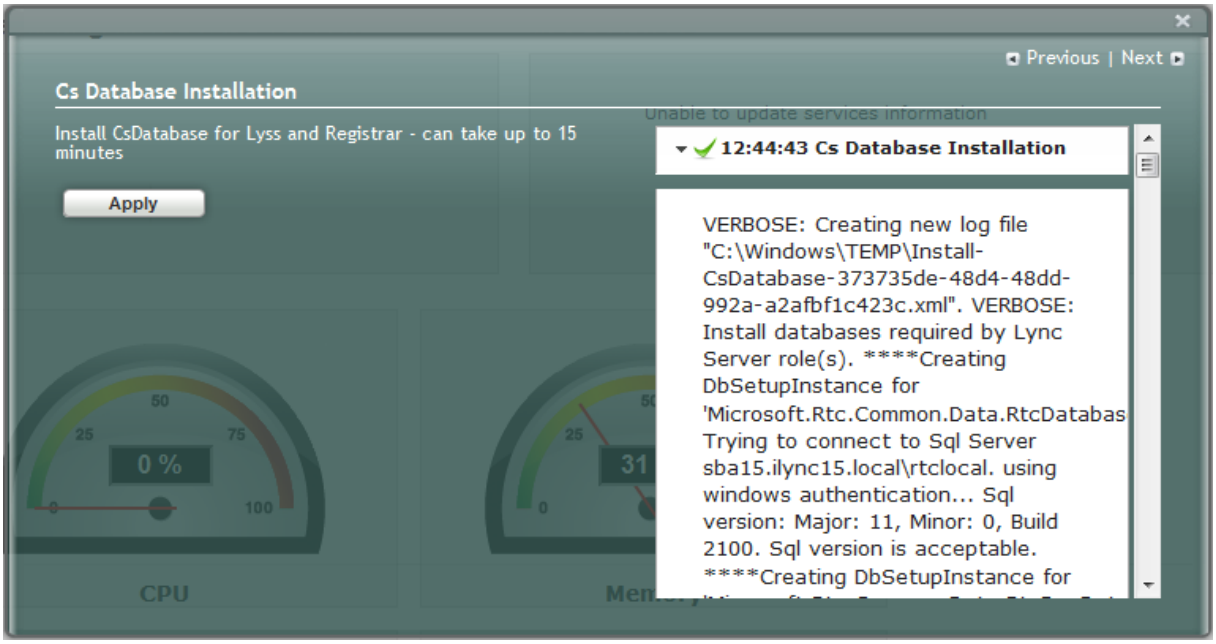
1. Under the **Setup** menu, click the **Cs Database installation** option; the following screen appears:

Figure 7-39: Cs Database installation Screen



2. Click **Apply**; the following screen appears:

Figure 7-40: Cs Database installation – Applied Successfully



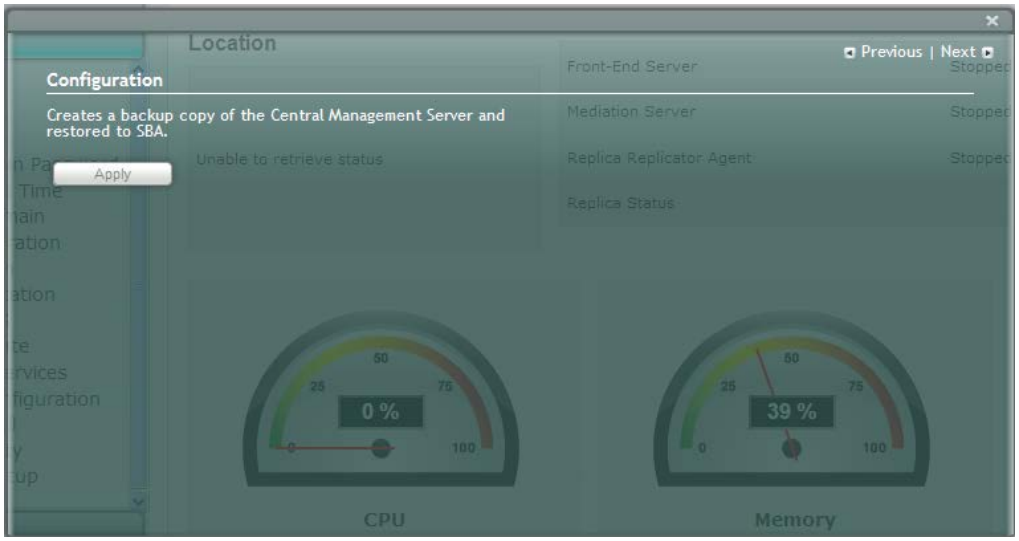
7.8 Step 8: Configuration

The **Configuration** option creates a backup copy of the Central Management Server on the SBA server.

➢ **To create a backup of the Central Management Server:**

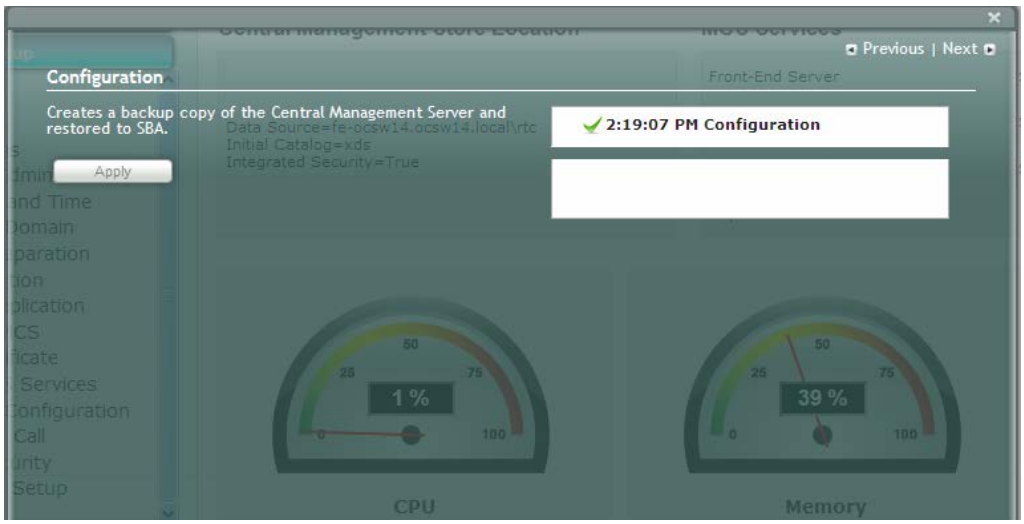
1. Under the **Setup** menu, click the **Configuration** option; the following screen appears:

Figure 7-41: Configuration Screen



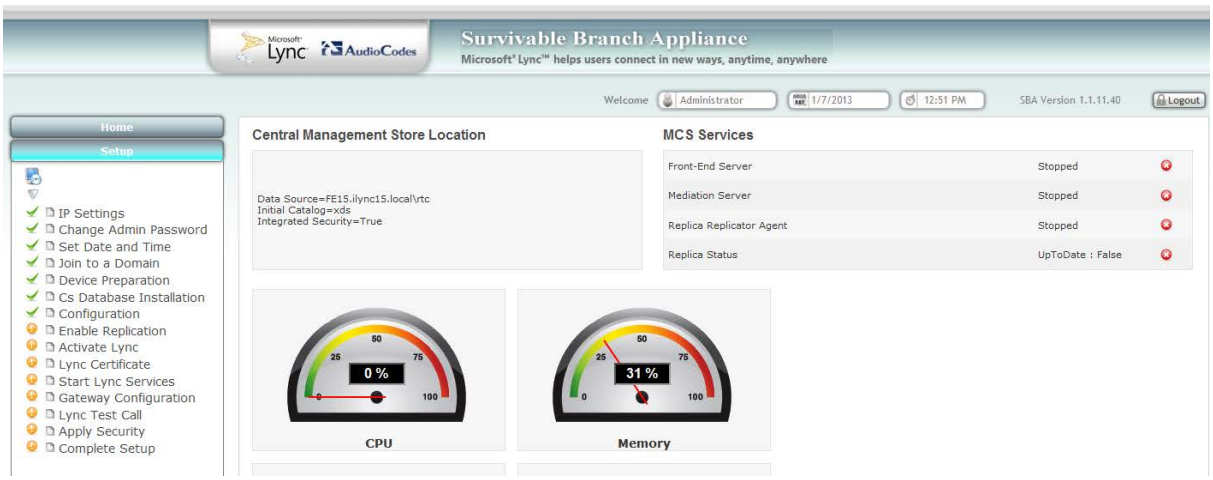
2. Click **Apply**; the following screen appears:

Figure 7-42: Configuration – Applied Successfully



A green check mark appears alongside the **Configuration** option under the **Setup** menu, as shown below:

Figure 7-43: Configuration – Completed Successfully



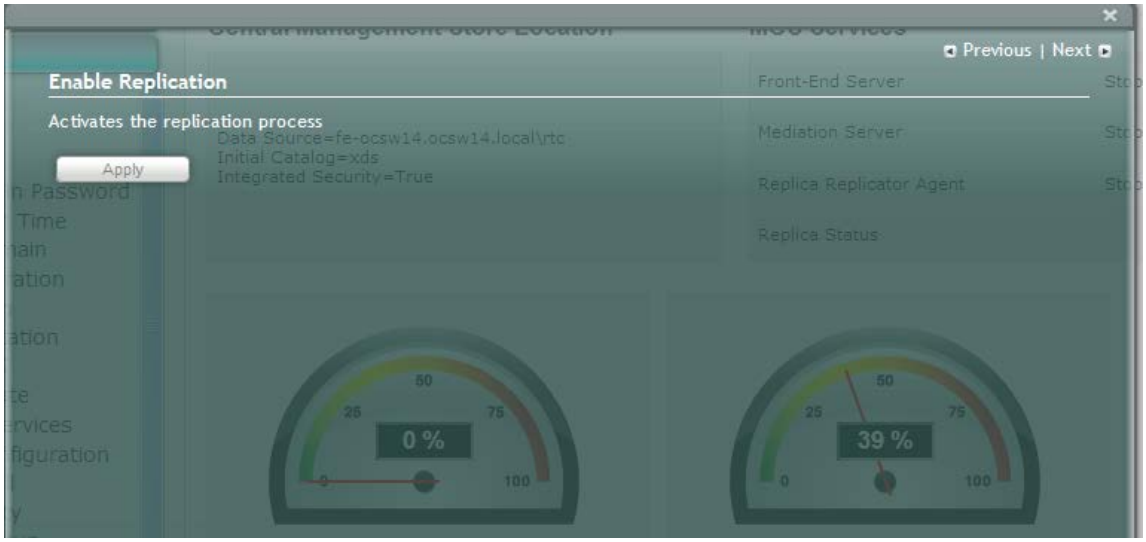
7.9 Step 9: Enable Replication

The **Enable Replication** option activates the replication process for the Lync Server 2013.

➢ **To enable replication:**

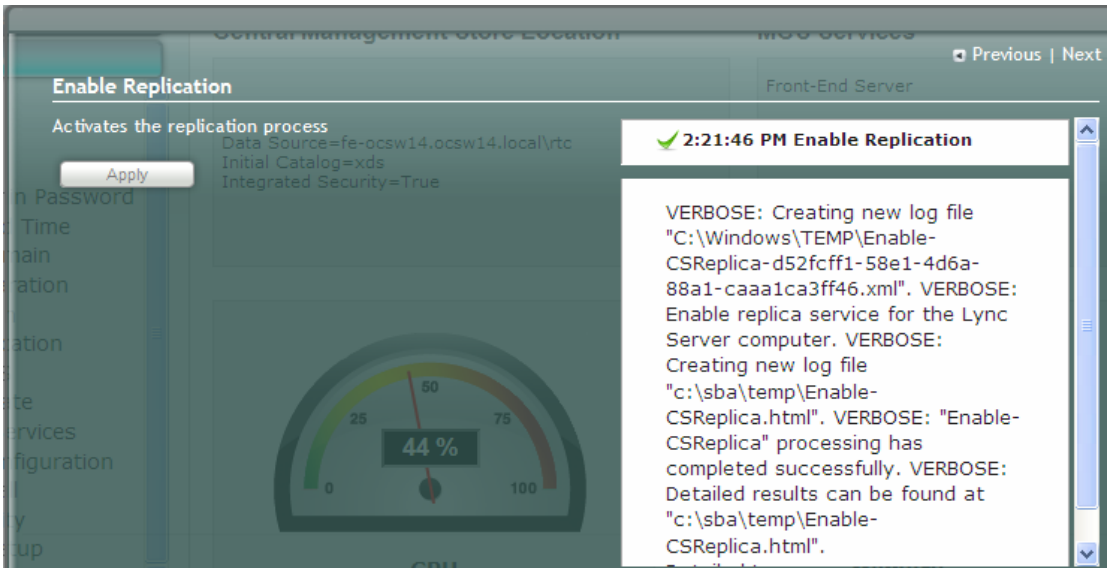
1. Under the **Setup** menu, click the **Enable Replication** option; the following screen appears:

Figure 7-44: Enable Replication Screen



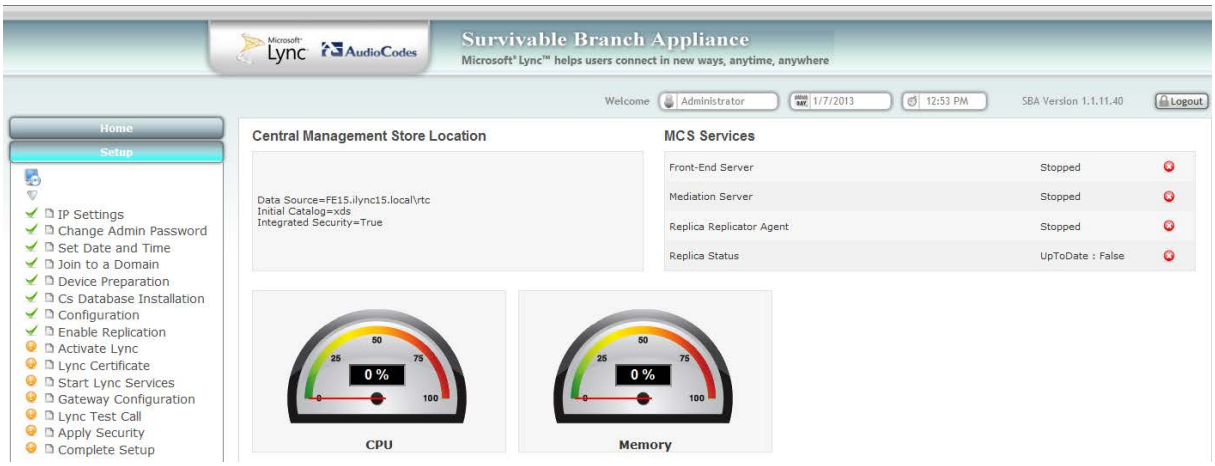
2. Click **Apply**; the following screen appears:

Figure 7-45: Enable Replication – Applied Successfully



A green check mark appears alongside the **Enable Replication** option under the **Setup** menu, as shown below:

Figure 7-46: Enable Replication – Completed Successfully



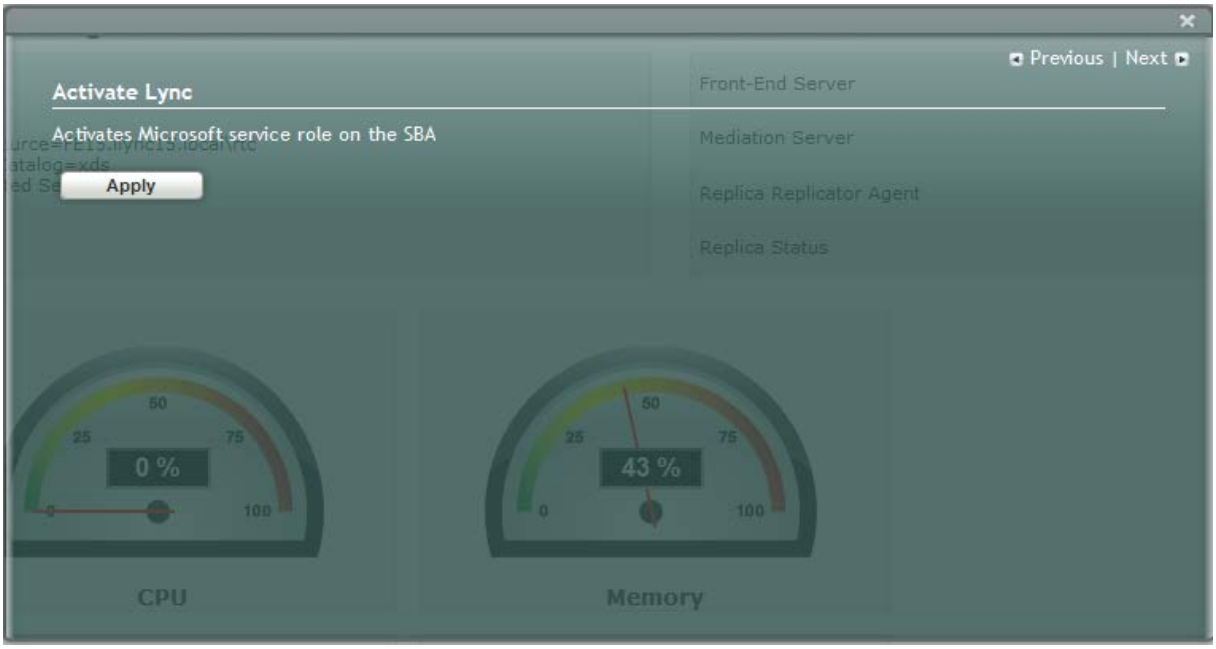
7.10 Step 10: Activate Lync

The **Activate Lync** option activates a computer running a Lync Server 2013 service role. Installing the required software does not automatically cause a computer to adopt a new service role; instead, that computer must be activated before it actually begins to function in its new role.

➢ **To activate Lync:**

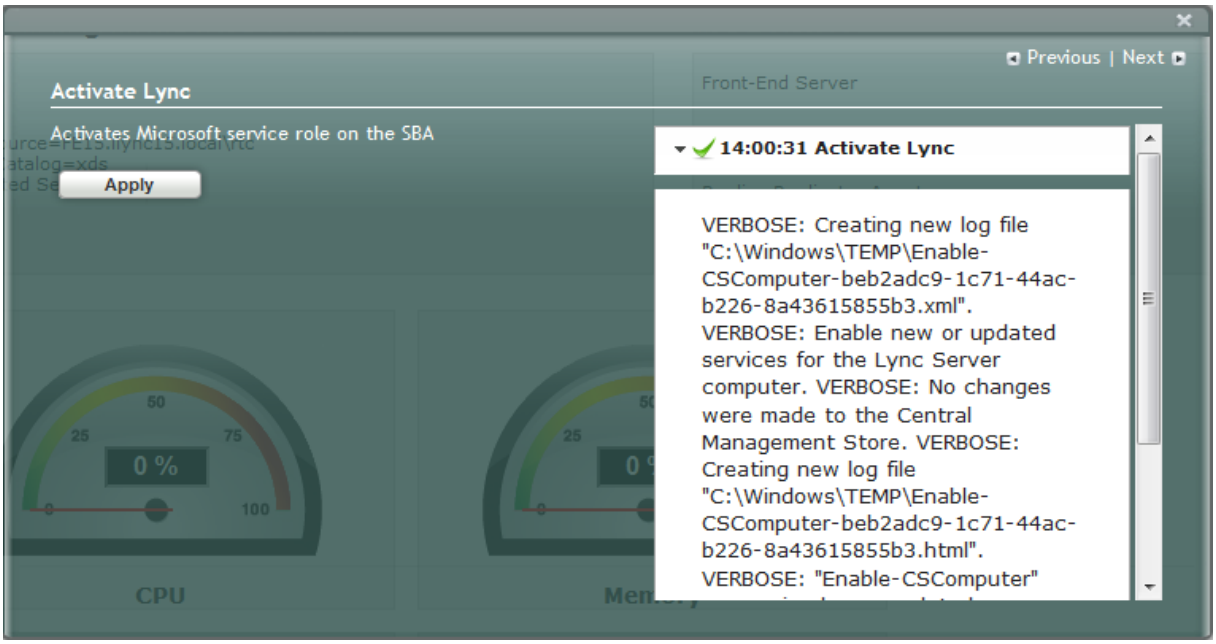
1. Under the **Setup** menu, click the **Activate Lync** option; the following screen appears:

Figure 7-47: Activate Lync Screen



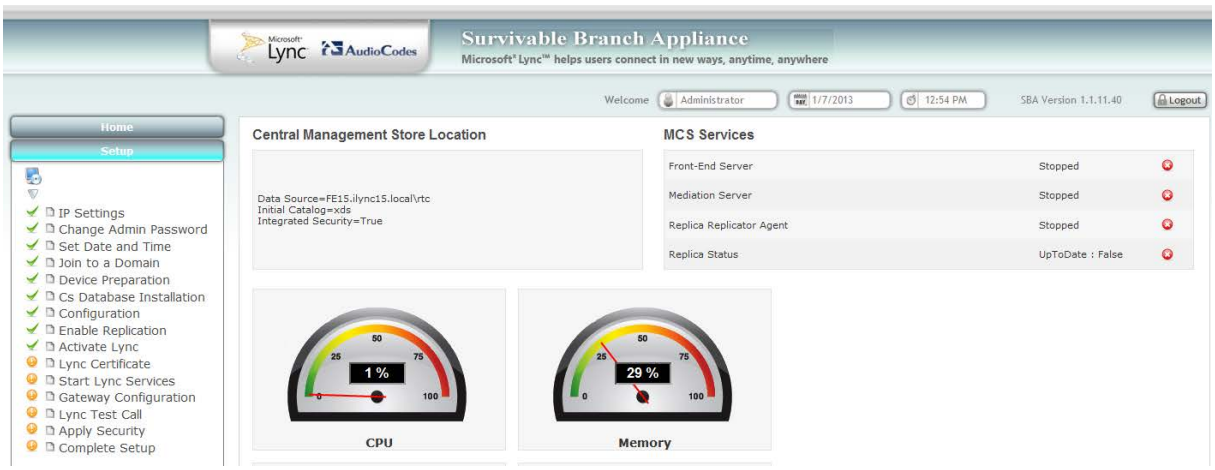
2. Click **Apply**; the following screen appears:

Figure 7-48: Activate Lync – Applied Successfully



A green check mark appears alongside the **Activate Lync** option under the **Setup** menu, as shown below:

Figure 7-49: Activate Lync – Completed Successfully



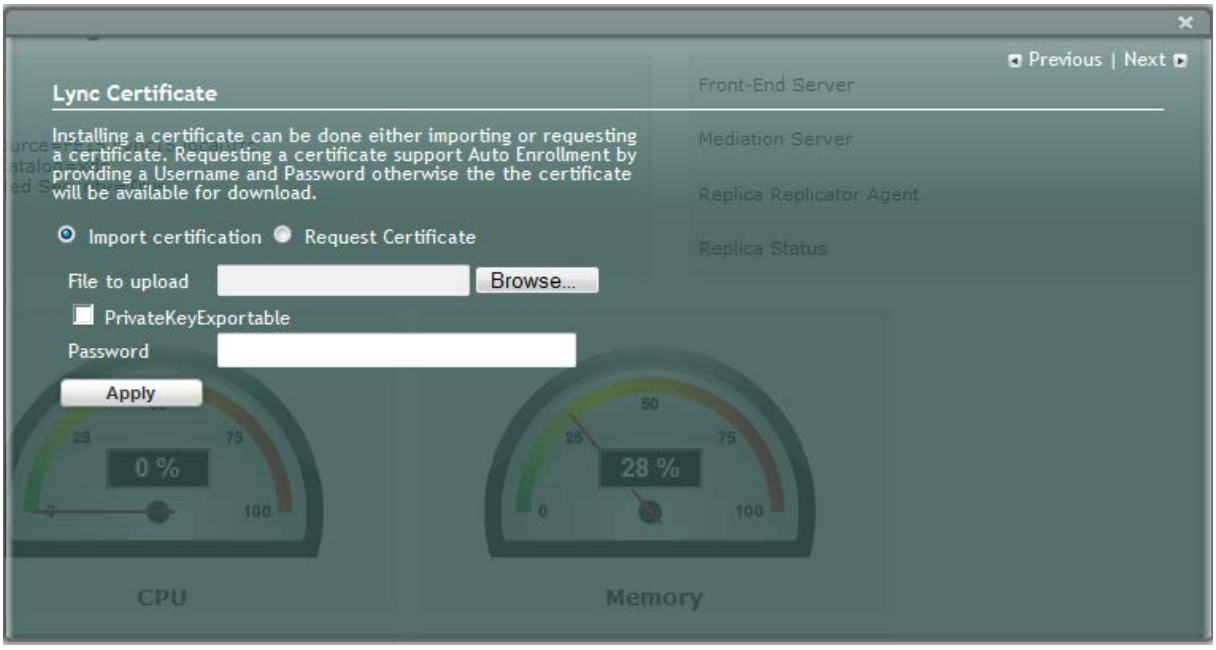
7.11 Step 11: Lync Certificate

The **Lync Certificate** option installs a certificate from the domain's certificate authority.

➢ **To install a Certificate:**

- Under the **Setup** menu, click the **Lync Certificate** option; the following screen appears:

Figure 7-50: Lync Certificate Screen



Certificates can be installed either by importing an existing certificate or requesting a new certificate.

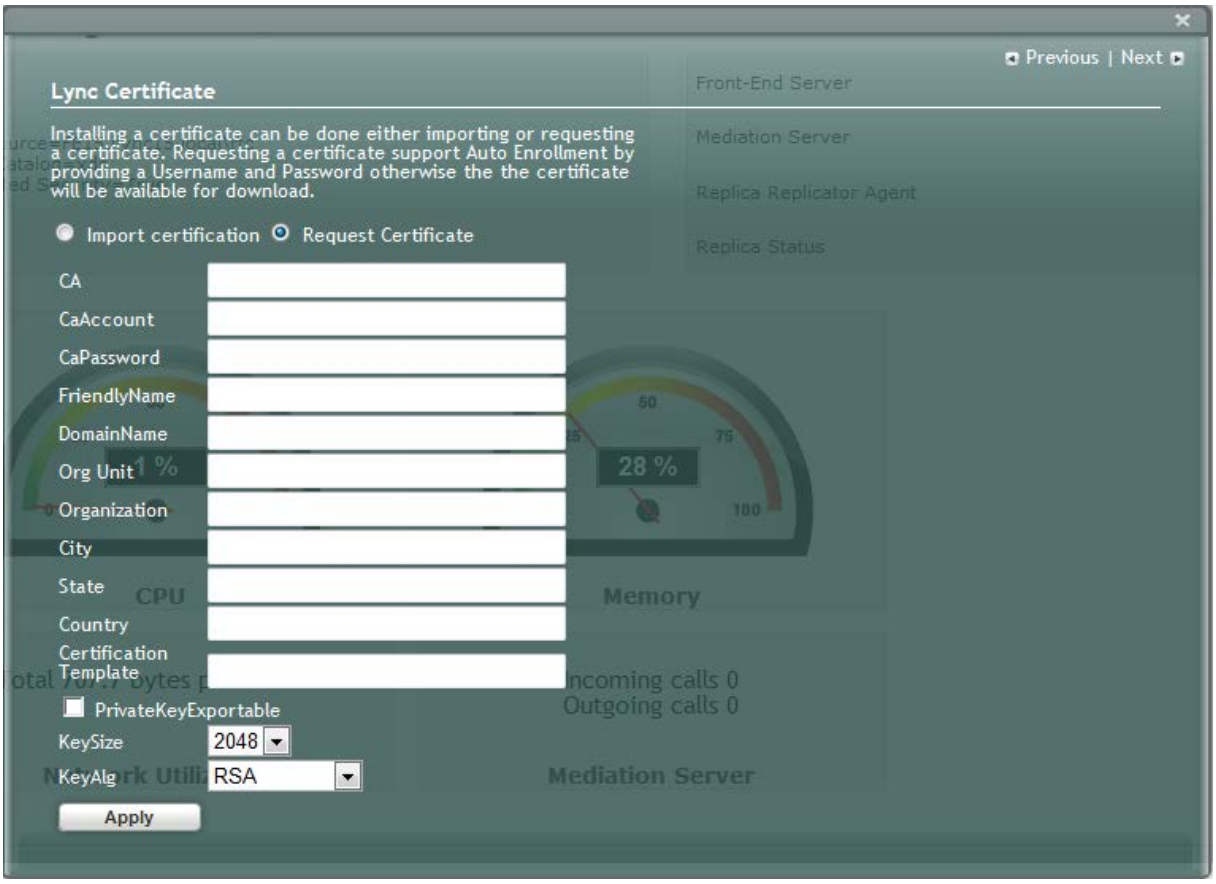
➢ **To import an existing certificate:**

1. Select the **Import Certification** radio button.
2. Click **Browse** to select the **File to Upload**.
3. Enter the **Password** (optional) of the certificates.
4. Click **Apply**.

➢ **To request a new certificate:**

1. Select the **Request Certificate** radio button.

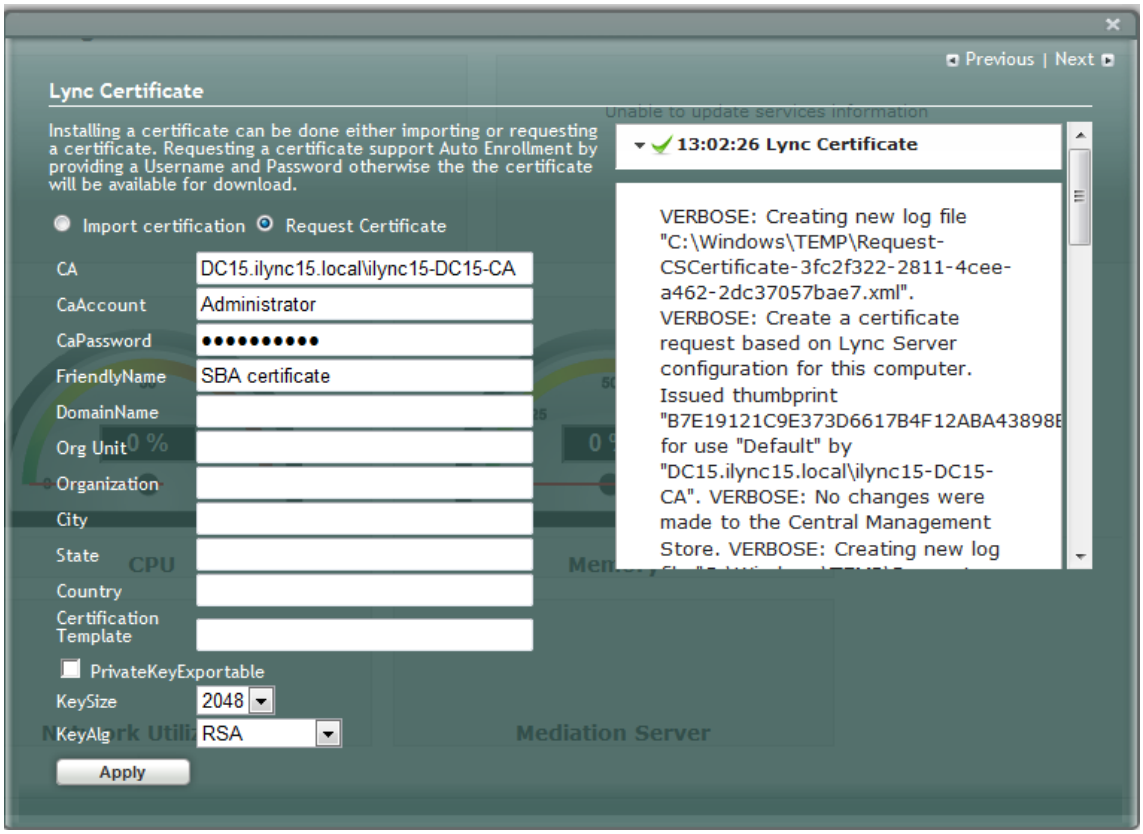
Figure 7-51: Request Certificate



2. Requesting a certificate supports Auto-enrollment. Enter all fields. Those fields beginning with a CA prefix are mandatory. The correct Certificate Authority (CA), User and Password must also be supplied.

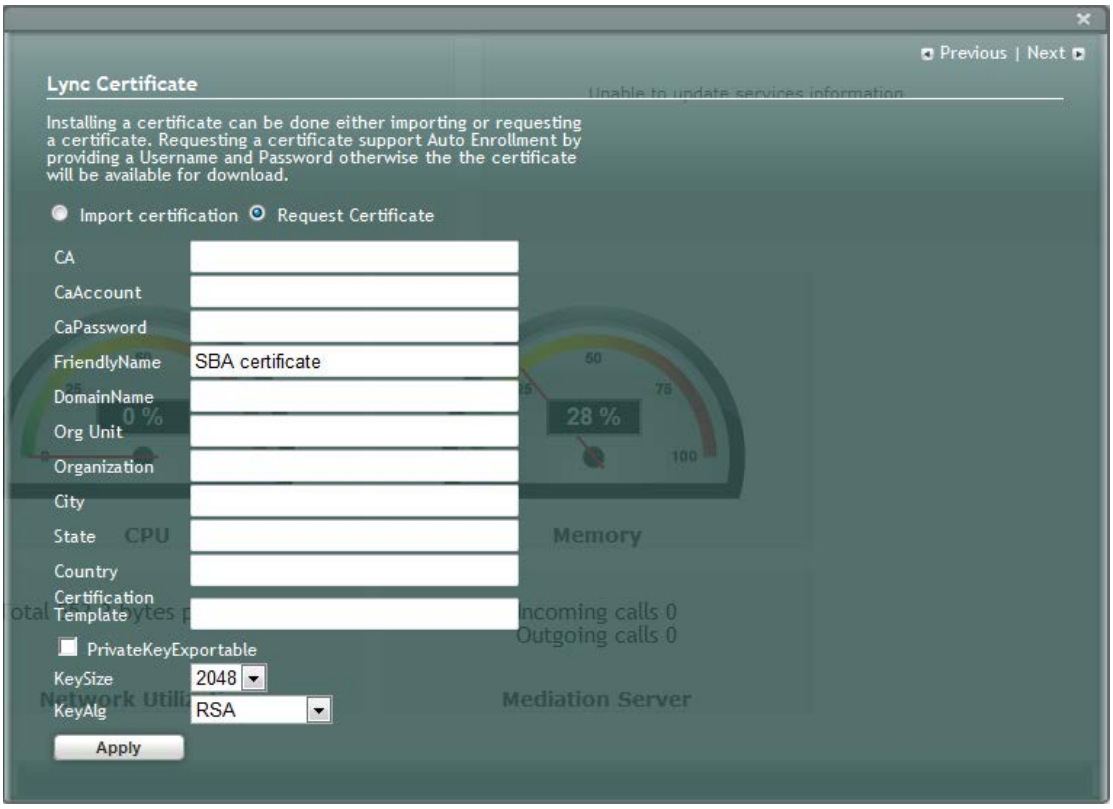
   The CA field contains the *<CA FQDN>\<CA Name> (e.g., CA.Lync.local\CA-DC-Lync-CA).*

Figure 7-52: Lync Certificate – Detailed Log



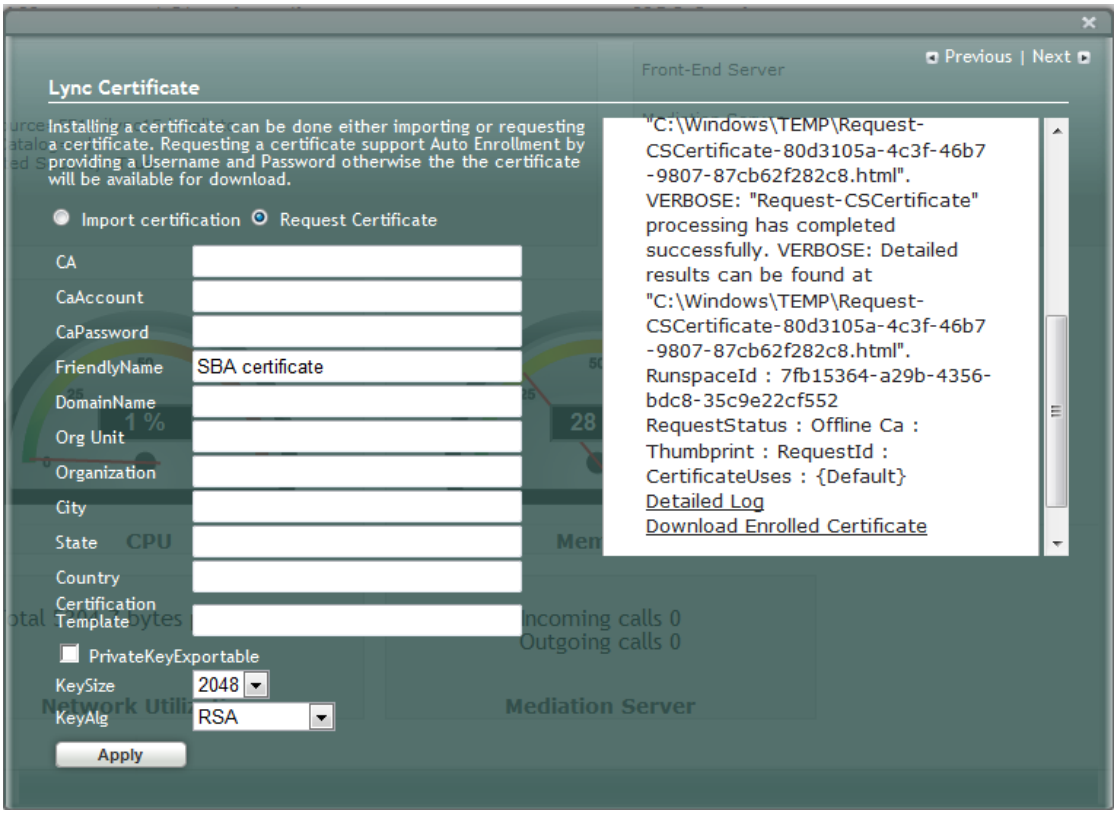
3. If the CA field is not entered, the system creates an enrollment certificate, which can be downloaded.

Figure 7-53: Lync Certificate – Download Enrolled Certificate



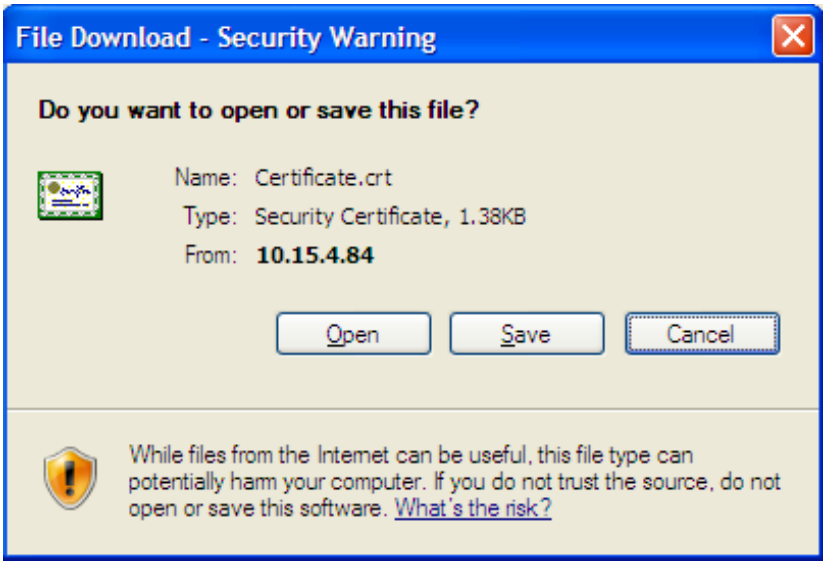
4. Click **Apply**; the following screen appears.

Figure 7-54: Lync Certificate – Download Enrolled Certificate



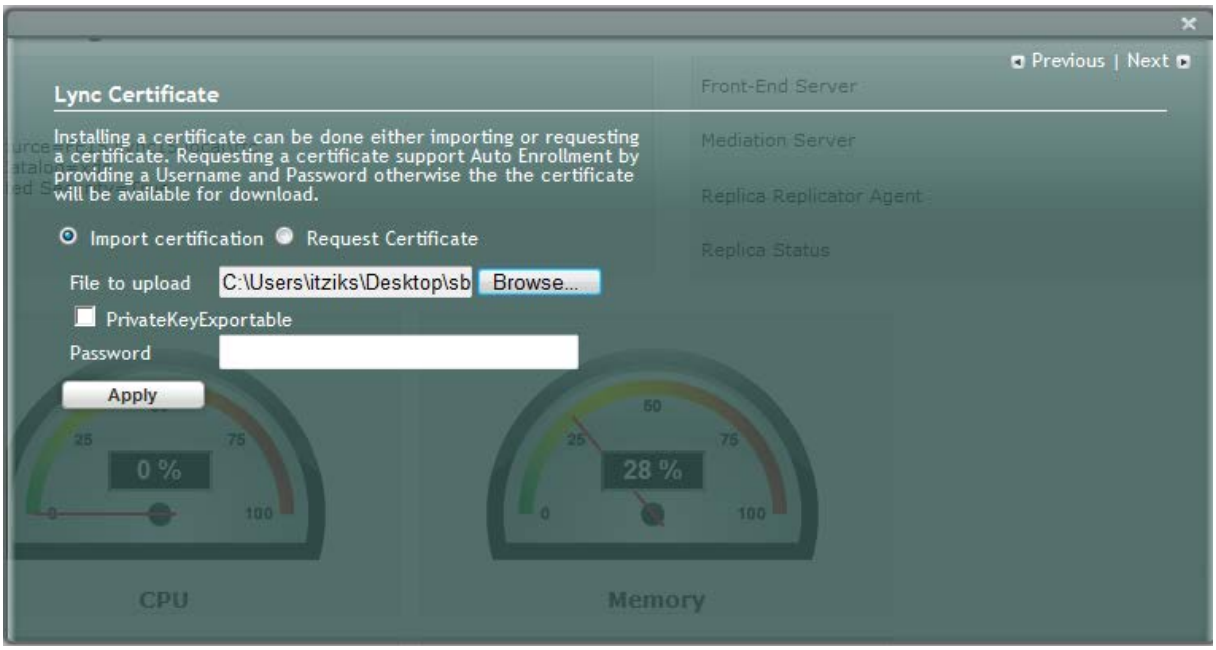
5. Click the **Download Enrolled Certificate** link**;** the following screen appears.

Figure 7-55: Lync Certificate – File Download



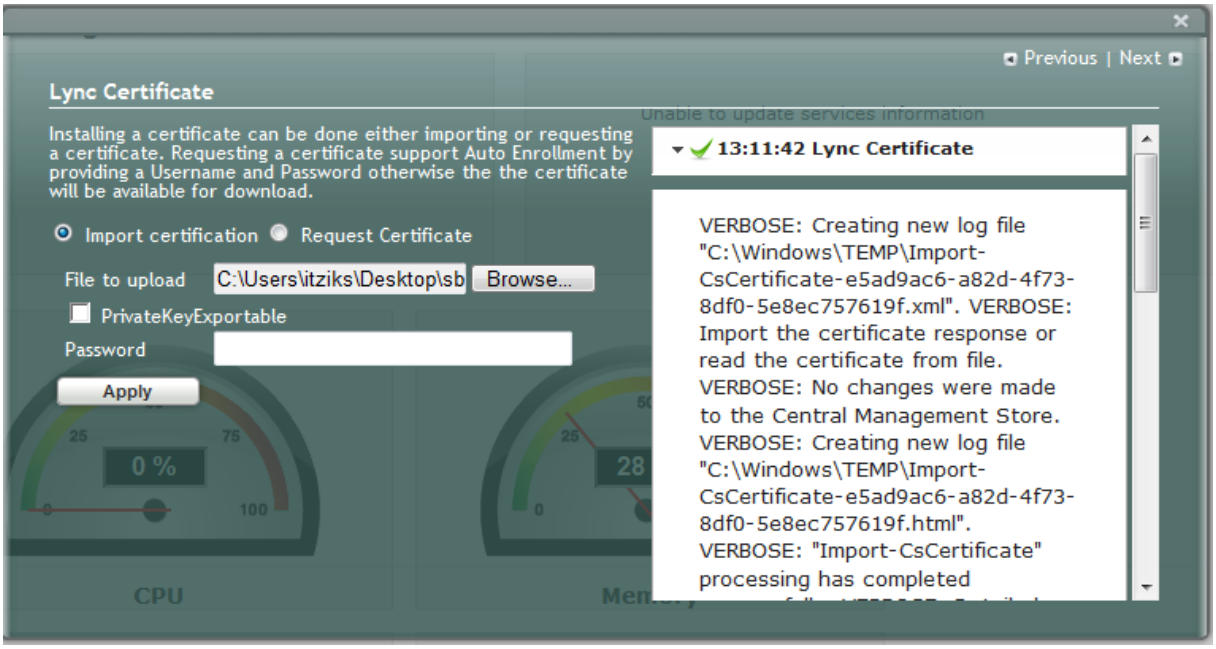
6. Click **Save**.
7. Once the Enrollment Certificate has been signed, select the **Import Certification** radio button as shown below and upload the signed certificate to be uploaded by using the **Browse** and **File to Upload** fields.

Figure 7-56: Lync Certificate – File Upload



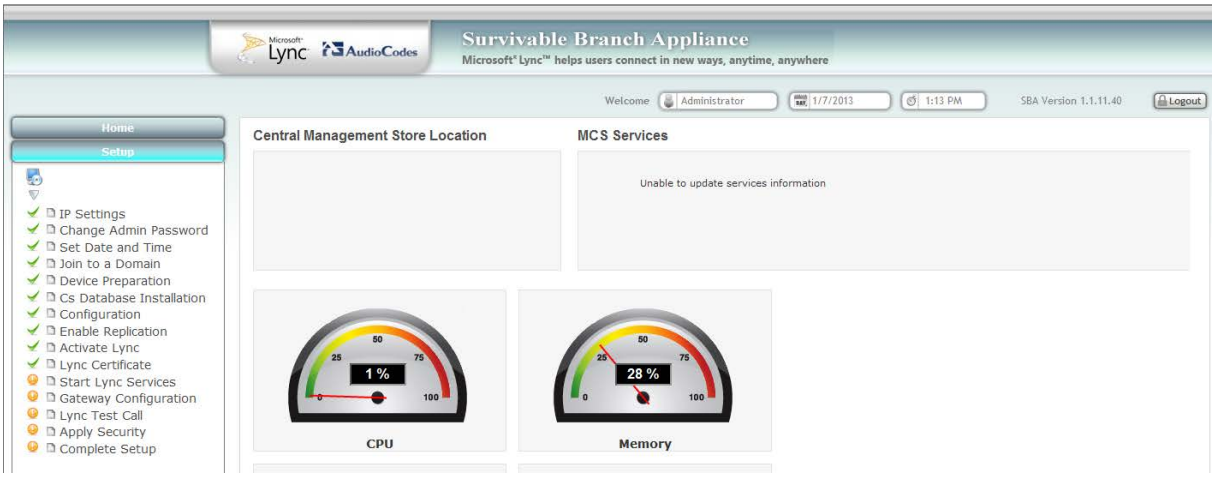
8. Click **Apply**; the following screen appears:

Figure 7-57: Lync Certificate – Detail Log



A green check mark appears adjacent to the completed menu item.

Figure 7-58: Lync Certificate – Complete



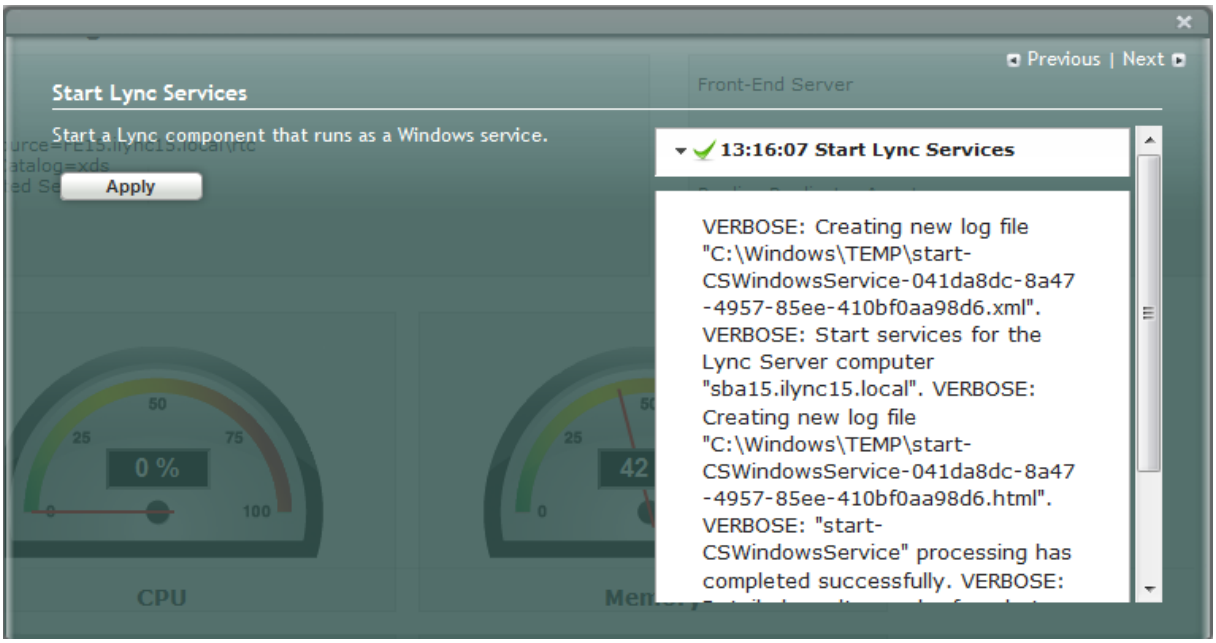
7.12 Step 12: Start Lync Services

The **Start Lync Services** option enables you to start a Lync Server 2013 (formerly, termed *Communications Server*) component that runs as a Windows service.

➢ **To start Lync services:**

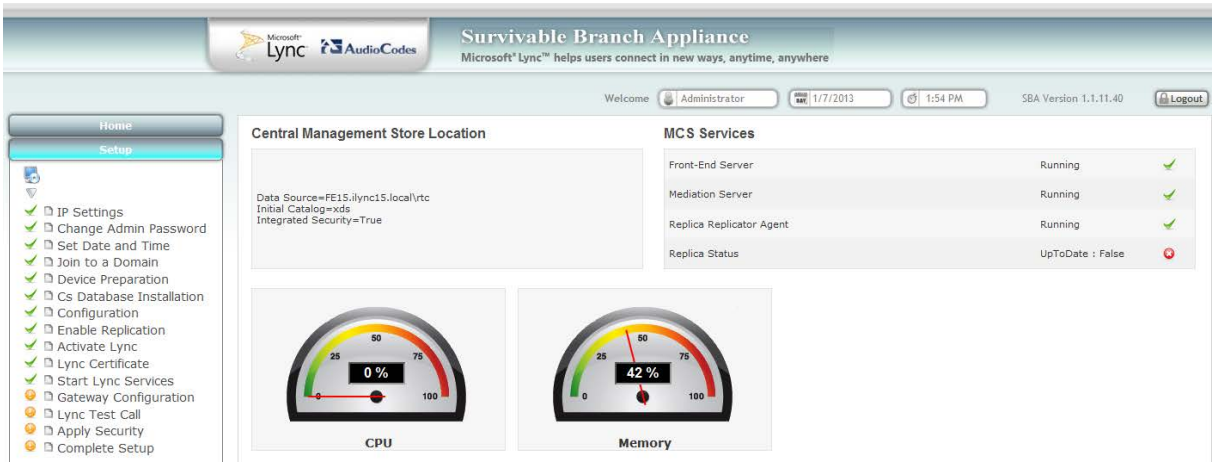
1. Under the **Setup** menu, click the **Start Lync Services** option; the following screen appears:

Figure 7-59: Start Lync Services Screen



2. Click **Apply** to start the services as per the Lync configuration settings; a green check mark appears alongside the **Start Lync Services** option under the **Setup** menu, as shown below:

Figure 7-60: Start Lync Services – Completed Successfully



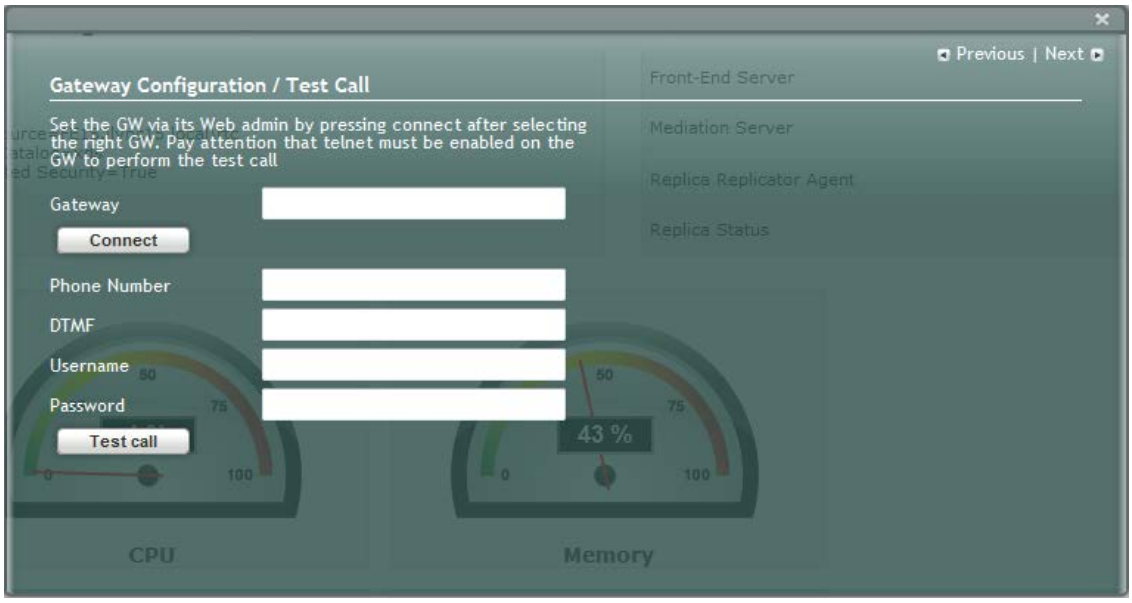
7.13 Step 13: Gateway Configuration

The **Gateway Configuration** option connects you to the Web-based interface of the PSTN Gateway functionality of Mediant 1000B SBA.

➢ **To configure the gateway:**

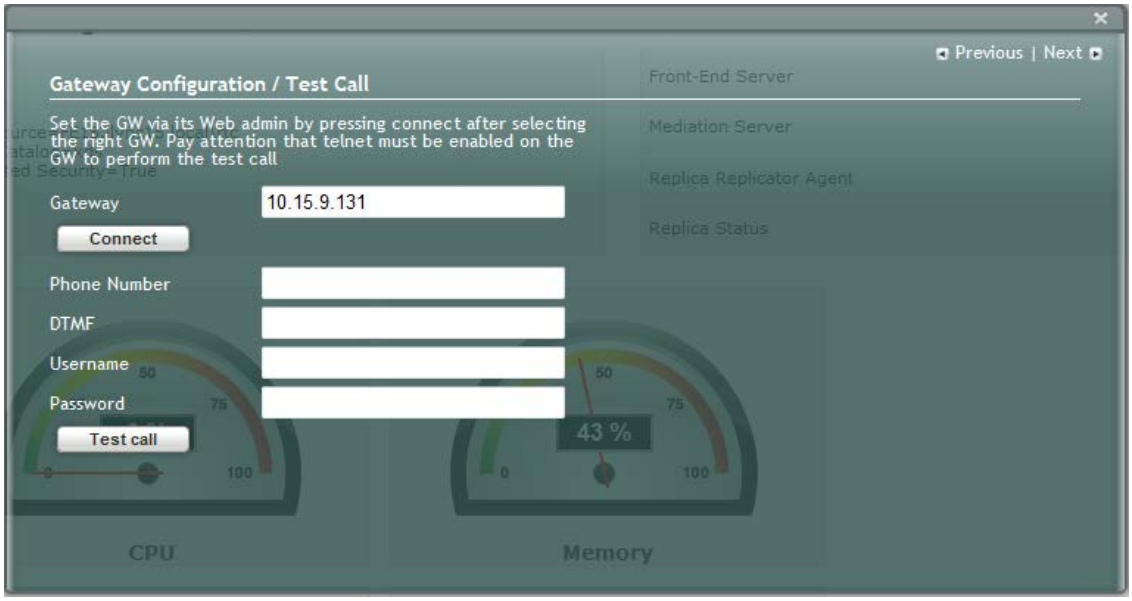
1. Under the **Setup** menu, click the **Gateway Configuration** option; the following screen appears:

Figure 7-61: Gateway Configuration Screen



2. In the 'Gateway' field, enter the IP address or DNS name of the Mediant 1000B, as shown below:

Figure 7-62: Gateway Configuration



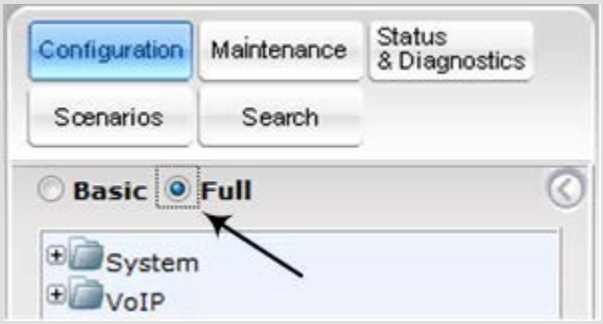
3. Click **Connect**.
4. Configure the PSTN Gateway as described in Section 8 on page 101.

8 Configuring the PSTN Gateway

This section provides step-by-step procedures for configuring the PSTN Gateway functionality of the Mediant 1000B SBA located at the branch office. The configuration is done through the embedded Web server (*Web interface*) of the PSTN Gateway.

Note: Before configuring the PSTN Gateway, ensure the following:

- The PSTN Gateway is running latest GA 6.60A SIP firmware Version.
- The PSTN Gateway must be installed with the following Feature Keys:
  - **MSFT** - enables working with Microsoft Lync
  - **IPSEC**, **MediaEncryption**, **StrongEncryption**, and **EncryptControlProtocol** - enable working with TLS
  - Before beginning to configure the E-SBC, select the **Full** option in the Web interface to display the full Navigation tree:



  When the E-SBC is reset, the Web interface reverts to **Basic** display.
  - This document applies to Microsoft Lync 2013 *and* to Microsoft Lync 2010.

8.1 Configuring the Mediation Server

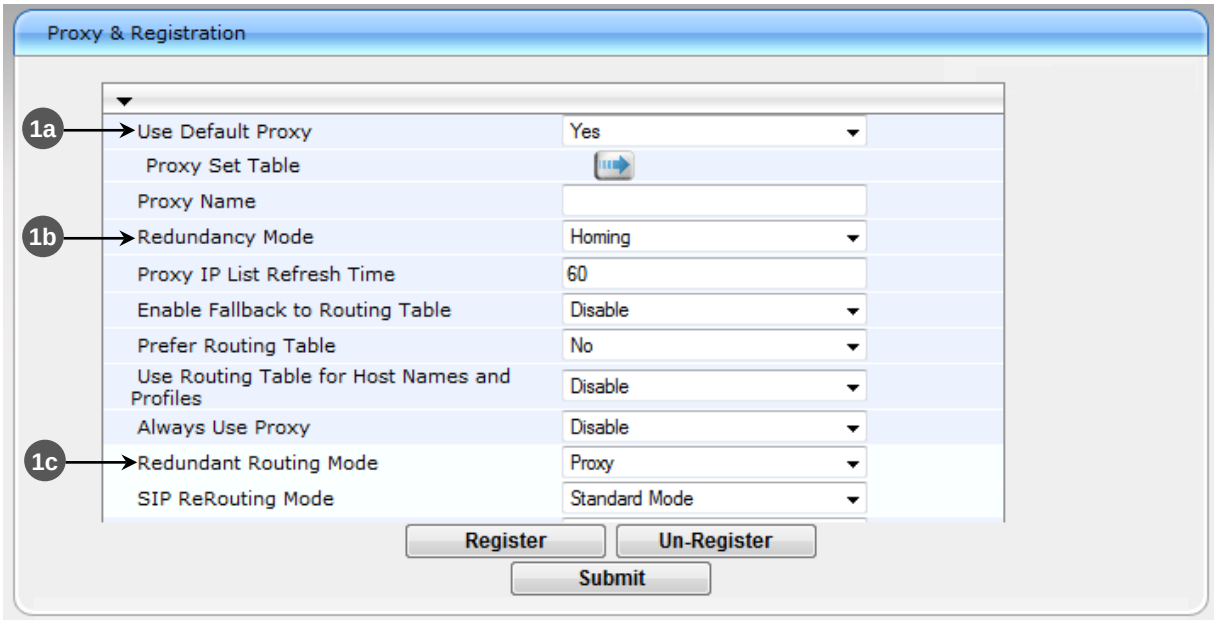
The procedure below describes how to configure the address (IP address or FQDN) of the Mediation Server through which the PSTN Gateway communicates with Lync. The PSTN Gateway forwards all telephone calls (PBX/PSTN and analog devices) to the Mediation Server using this configured address. The address is configured in the PSTN Gateway as a proxy server. In other words, the Mediation Server acts as a proxy server (without registration) for the PSTN Gateway.

If you have more than one Mediation Server in the cluster, proxy redundancy functionality can also be configured. If the Mediation Server running on the Mediant 1000B SBA is unavailable (i.e., a SIP 503 is received in response to an INVITE), then the PSTN Gateway re-sends the INVITE to the next Mediation Server (located at the datacenter).

➢ **To configure the Mediation Server:**

1. Open the Proxy & Registration page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Proxy & Registration**).

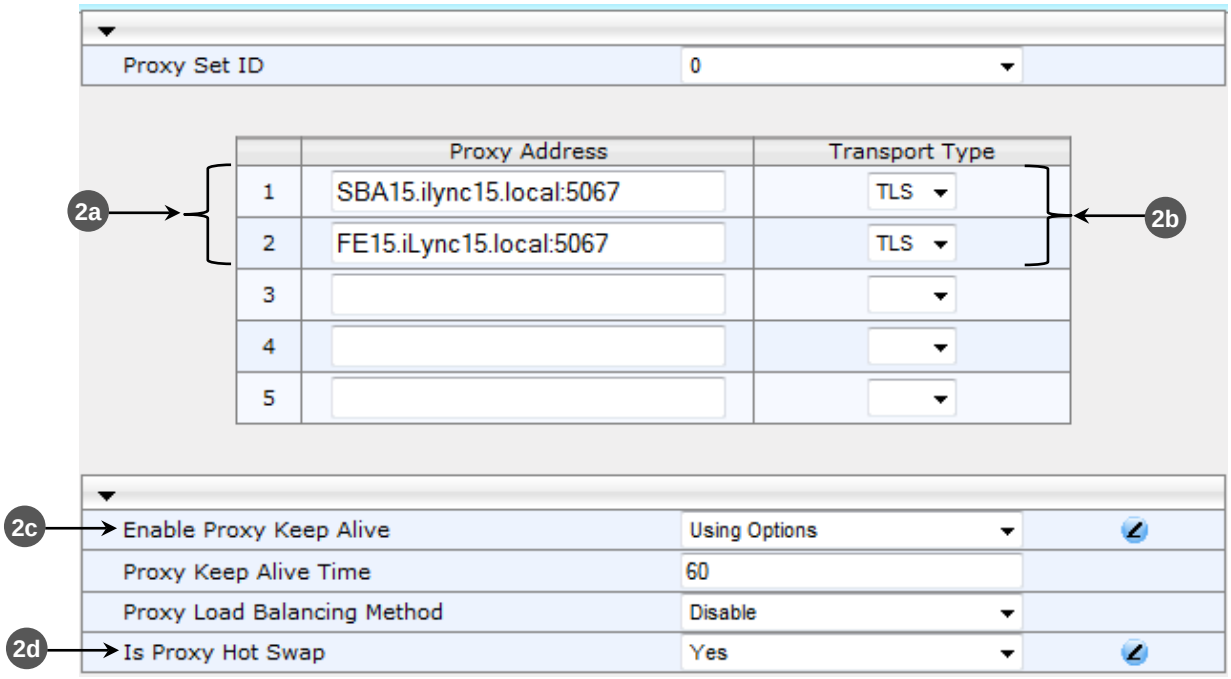
Figure 8-1: Proxy & Registration Page



a. From the 'Use Default Proxy' drop-down list, select **Yes** to enable the Mediation Server to serve as a proxy server.
b. From the 'Redundancy Mode' drop-down list, select **Homing**. If the SBA application fails and the PSTN Gateway switches over to the Mediation Server at the datacenter, then when the SBA application resumes functionality again, the PSTN Gateway switches back to the Mediation Service on the SBA application.
c. From the 'Redundant Routing Mode' drop-down list, select **Proxy**. This setting ensures that if a SIP 5xx message is received in response to an INVITE message sent to the primary proxy (i.e., Mediation Server on the Mediant 1000B SBA), the PSTN Gateway re-sends it to the redundant proxy (i.e., Mediation Server at the datacenter). To configure alternative routing upon receipt of a SIP 503 response (as required by Lync), see Step 3 on page 104.
d. Click **Submit**.

2. Click the **Proxy Set Table** button to open the 'Proxy Sets Table' page:

Figure 8-2: Proxy Sets Table Page



a. In the 'Proxy Address' fields, configure two proxy servers for redundancy. If the SBA application fails (at the branch office), the PSTN Gateway switches over to the Mediation Server located at the datacenter.
   - **Index 1:** IP address or FQDN of the Mediation Server running on the Mediant 1000B SBA (configured in Section 8.3.1.4 on page 109).
   - **Index 2:** IP address or FQDN of the Mediation Server running at the datacenter.

Note: If you configured the Mediation Server address as an FQDN, ensure that you configure the DNS server (see Section 8.3.1.2 on page 108).

b. In the 'Transport Type' drop-down list, select the Transport Type (TLS or TCP) for these proxies. For more information on TLS and TCP Transport Type configuration, see Section 8.3 on page 106.

c. From the 'Enable Proxy Keep Alive' drop-down list, select **Using Options** to discover whether a particular Mediation Server in the cluster is available.

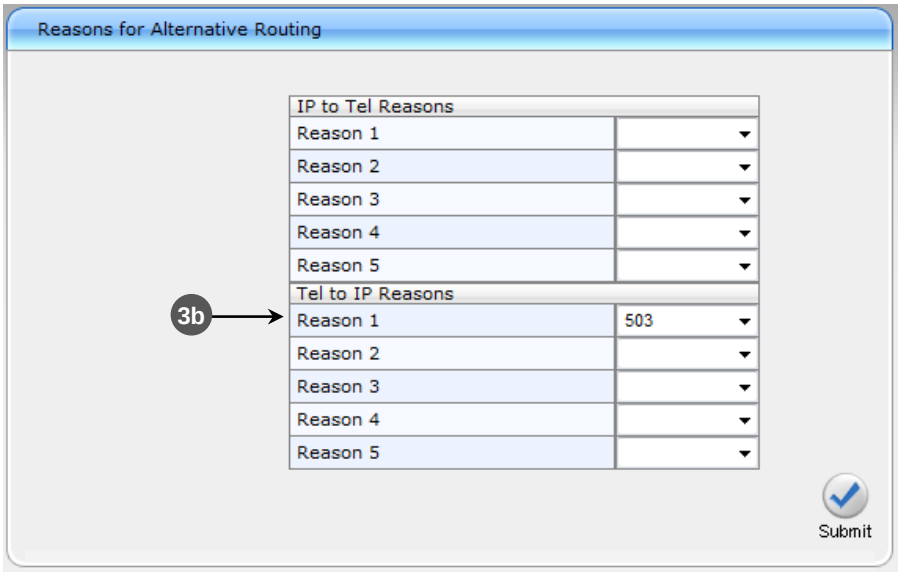
d. From the 'Is Proxy Hot Swap' drop-down list, select **Yes**. If there is no response from the first Mediation Server after a user-defined number of retransmissions, the INVITE message is sent to the redundant Mediation Server. The number of retransmissions is configured by the *Number of RTX Before Hot-Swap* parameter in the 'Proxy & Registration' page (see Step 1 on page 102).

e. Click **Submit** to apply your settings.

3. When the PSTN Gateway receives a SIP 503 response from the Mediation Server in response to an INVITE, it re-sends the INVITE to the redundant Mediation Server (located at the datacenter). To achieve this, you need to configure the receipt of a SIP 503 response as a reason for IP alternative routing:

   a. Open the 'Reasons for Alternative Routing' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Routing** > **Alternative Routing Reasons**).

Figure 8-3: Reasons for Alternative Routing Page

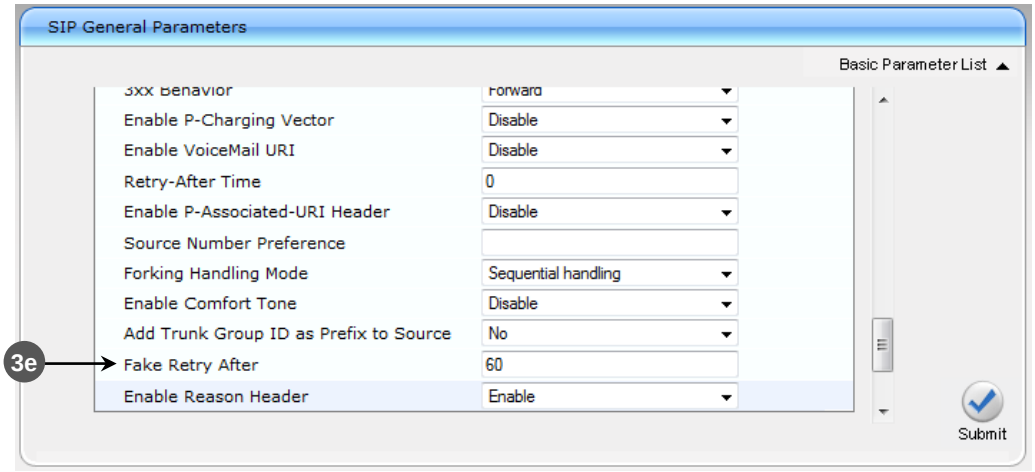


   b. Under the **Tel to IP Reasons** group, from the 'Reason 1' drop-down list, select **503**.

   c. Click **Submit**.

   d. Open the 'SIP General Parameters' page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **General Parameters**).

Figure 8-4: SIP General Parameters Page



   e. In 'Fake Retry After' field, enter the time '60' (in seconds). When the PSTN Gateway receives a SIP 503 response (from the Mediation Server) without a Retry-After header, the PSTN Gateway behaves as if the 503 response includes a Retry-After header with this user-defined period.

   f. Click **Submit**.

   g. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.

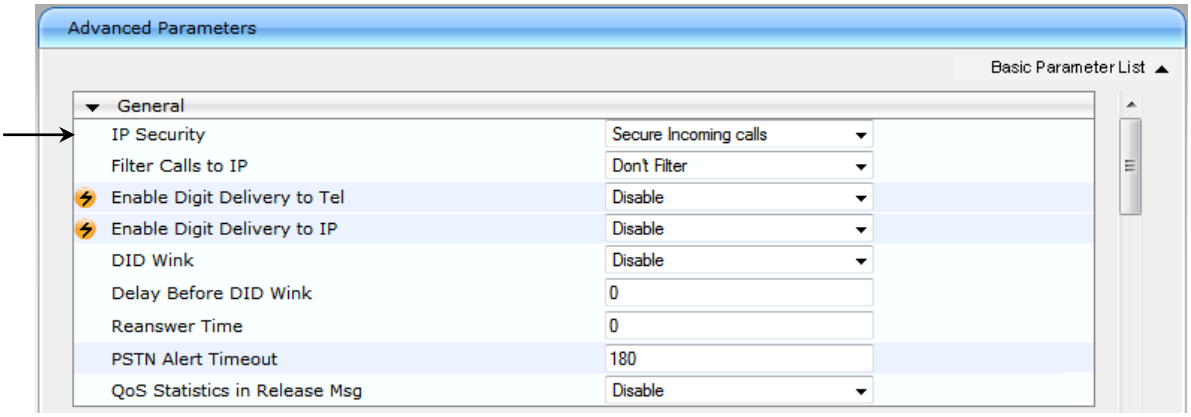
8.2 Restricting Communication to Mediation Server Only

The procedure below describes how to restrict IP communication, by allowing communication only between the PSTN Gateway and the Mediation Server. This ensures that the PSTN Gateway accepts and sends SIP calls **only** from and to the Mediation Server (as required by Microsoft). This is done by enabling the IP Security feature and then defining the allowed ("administrative" list) IP addresses (or FQDNs) in the Proxy Set table.

➢ **To allow IP communication only between the PSTN Gateway and Mediation Server:**

1. Open the Advanced Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Advanced Parameters**).

Figure 8-5: Advanced Parameters Page



2. From the 'IP Security' drop-down list, select 'Secure Incoming calls' to enable the security feature to accept and send SIP calls only from and to user-defined IP addresses or FQDN (i.e., Mediation server) configured in the 'Proxy Set table' (see Step 1).
3. Click **Submit** to apply your settings.
4. On the toolbar, click **Burn** to save the changes to the Enhanced gateway flash memory.

8.3 Configuring the SIP Transport Type

The following SIP transport types can be employed for communication between the PSTN Gateway and the Mediation Server:

- **Transport Layer Security (TLS)** – enabled by default (and recommended) - see Section 8.3.1 on page 106.
- **Transmission Control Protocol (TCP)** – see Section 8.3.2 on page 115.

8.3.1 Configuring TLS

TLS provides encrypted SIP signaling between the PSTN Gateway and the Mediation Server. When using TLS, you also need to configure the PSTN Gateway with a certificate for authentication during the TLS handshake with the Mediation Server.

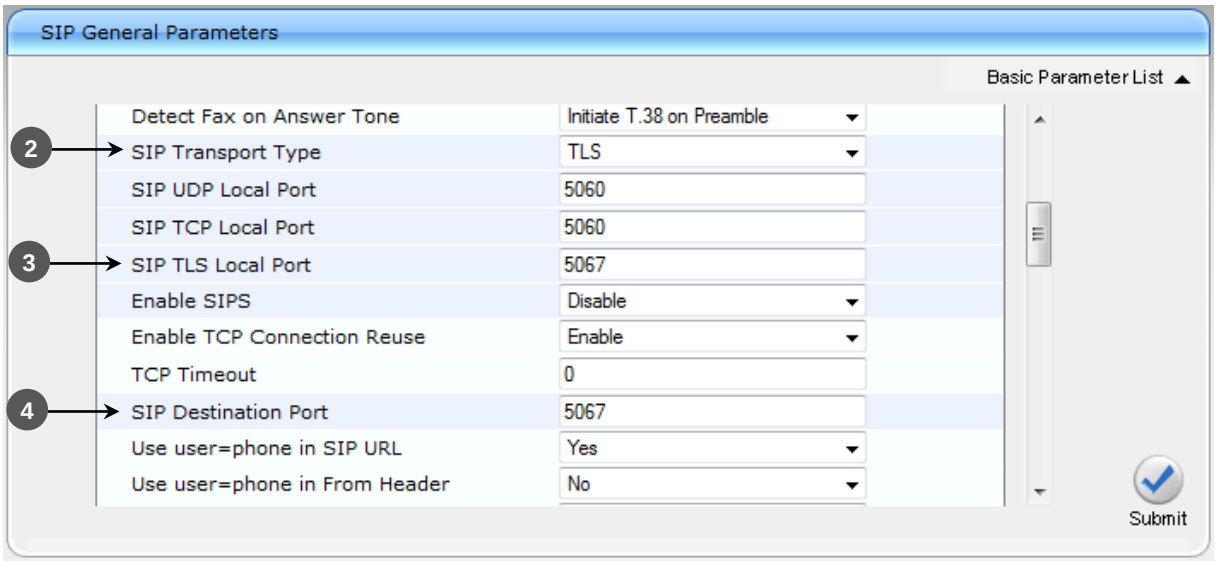
8.3.1.1 Step 1: Enable TLS and Define TLS Port

The procedure below describes how to enable TLS and configure the PSTN Gateway ports used for TLS.

➢ **To enable TLS and configure TLS ports:**

1. Open the SIP General Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **General Parameters**).

Figure 8-6: SIP General Parameters Page



2. From the 'SIP Transport Type' drop-down list, select **TLS**.
3. In the 'SIP TLS Local Port', enter "5067". This port corresponds to the Mediation Server TLS transmitting port configuration.
4. In the 'SIP Destination Port', enter "5067". This port corresponds to the Mediation Server TLS listening port configuration.
5. Click **Submit** to apply your settings.
6. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.

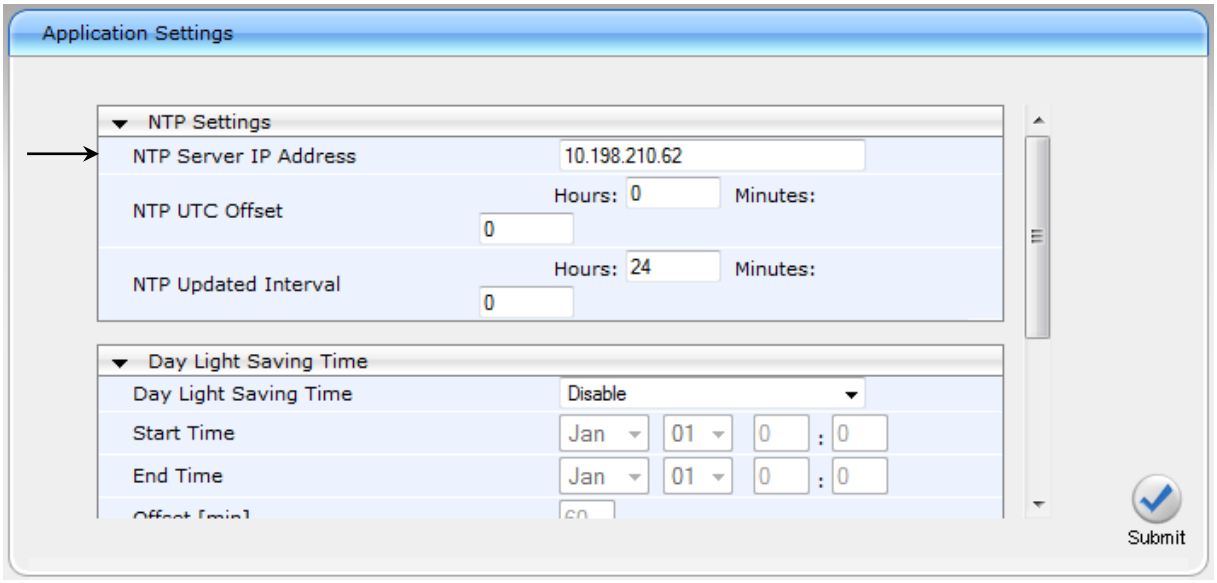
8.3.1.2 Step 2: Configure the NTP Server

The procedure below describes how to configure the Network Time Protocol (NTP) server. This is important for maintaining the correct time and date on the PSTN Gateway, by synchronizing it with a third-party NTP server. This ensures that the PSTN Gateway has the same date and time as the Certification Authority (CA), discussed later in Section 8.3.1 on page 106.

➢ **To configure the NTP server:**

1. Open the Application Settings page (**Configuration** tab > **System** menu > **Application Settings**).

Figure 8-7: Application Settings Page



2. In the 'NTP Server IP Address' field, enter the IP address of the NTP server.
3. Click **Submit** to apply your changes.
4. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.

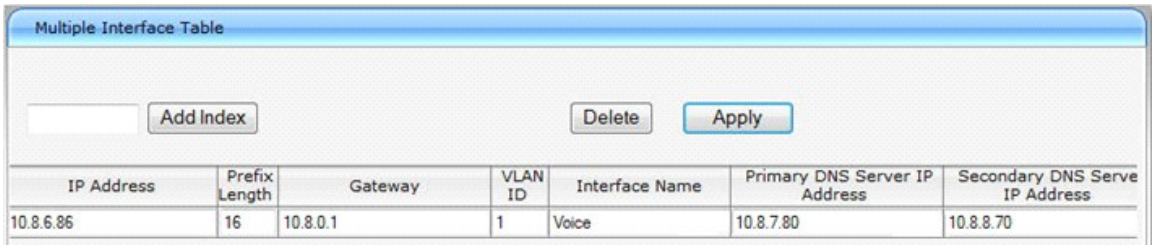
8.3.1.3 Step 3: Configure the DNS Server

The procedure below describes how to configure the IP address of the Domain Name System (DNS) servers. This is required if the Mediation Server is configured with an FQDN, in which case, the DNS is used to resolve it into an IP address.

➢ **To configure the DNS servers:**

1. Open the IP Settings page (**Configuration** tab > **VoIP** menu > **Network** > **IP Settings**).

Figure 8-8: DNS Server Settings



2. In the 'DNS Primary Server IP' and 'DNS Secondary Server IP' fields, enter the IP address of the primary and secondary DNS server, respectively.
3. Click **Submit** to apply your changes.
4. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.

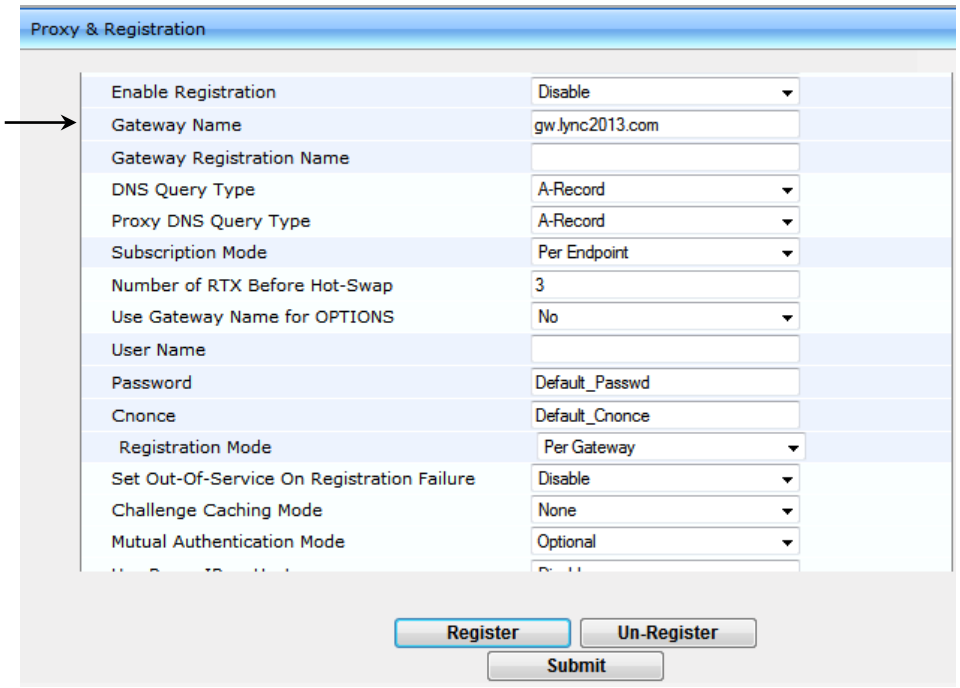
8.3.1.4 Step 4: Configure the Gateway Name

The procedure below describes how to configure the host name for the PSTN Gateway. This appears as the URI host name in the SIP From header in INVITE messages sent by the PSTN Gateway to the Mediation Server. This allows the Mediation Server to identify the PSTN Gateway (if required), when using certificates for TLS (see Section 8.3.1.5.1 on page 110).

➢ **To configure the SIP gateway name:**

1. Open the Proxy & Registration page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Proxy & Registration**).

Figure 8-9: Proxy & Registration Page



2. In the 'Gateway Name' field, assign a unique FQDN name to the PSTN Gateway within the domain, for example,'gw.lync2013.com'.This name is identical to the name that is configured in the Lync topology builder (see Section 5.2.1 on page 49).
3. Click **Submit** to apply your settings.
4. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.

8.3.1.5 Step 5: Configure a Certificate

This step describes how to exchange a certificate with Microsoft Certificate Authority (CA). It is composed of the following steps:

1. Generating a certificate signing request (CSR).
2. Obtaining CA and Trusted Root certificates from Microsoft.
3. Installing Microsoft CA and Trusted Root certificates on the PSTN Gateway.

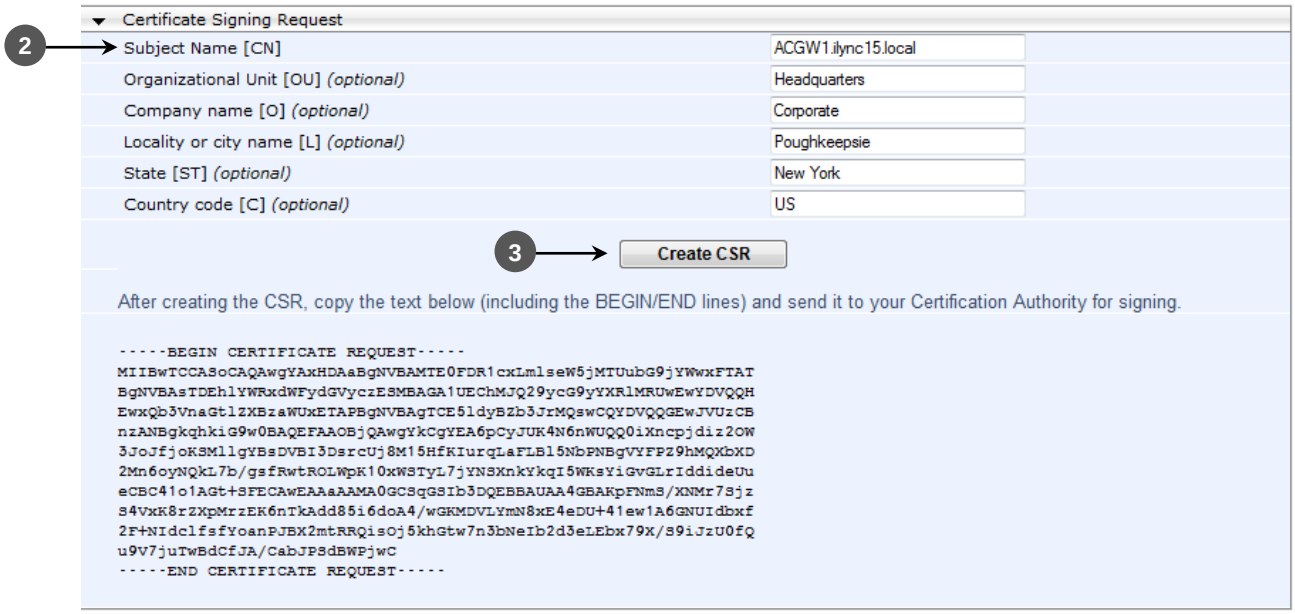
8.3.1.5.1 Generate a Certificate Signing Request

The procedure below describes how to generate a CSR by the PSTN Gateway. This CSR is later sent to Microsoft CA.

➢ **To generate a CSR:**

1. Open the 'Certificates Signing Request' page (**Configuration** tab > **System** menu > **Certificates**).

Figure 8-10: Certificates Page



2. In the 'Subject Name' field, enter the SIP URI host name that you configured for the PSTN Gateway in Section 8.3.1.4 on page 109.
3. Click **Create CSR**; a Certificate request is generated and displayed on the page.
4. Copy the certificate from the line "----BEGIN CERTIFICATE" to "END CERTIFICATE REQUEST----" to a text file (such as Notepad), and then save it to a folder on your PC with the file name *certreq.txt*.

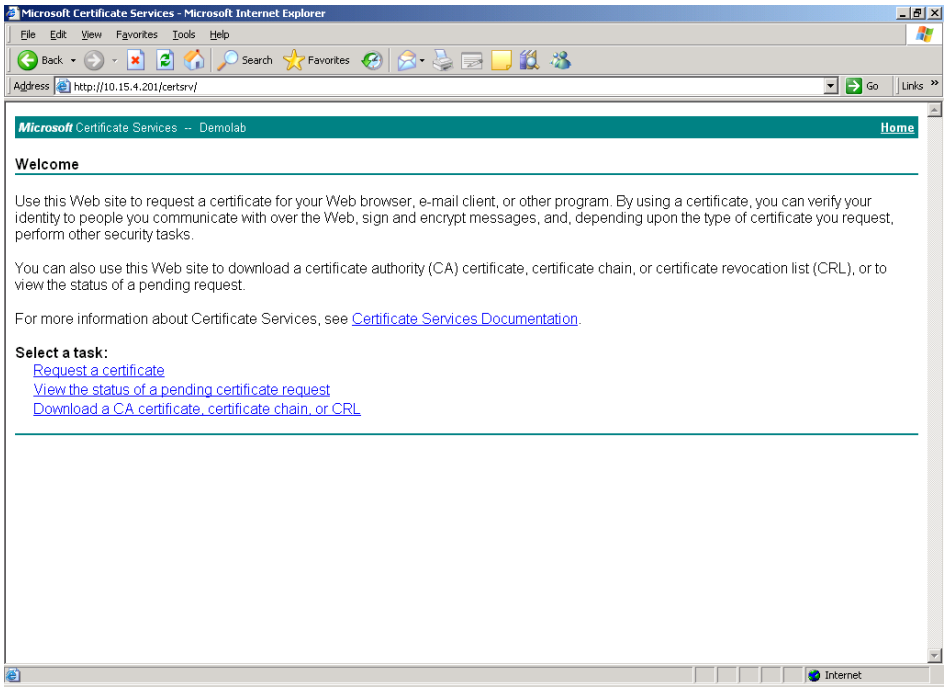
8.3.1.5.2 Obtain Microsoft CA and Trusted Root Certificates

Once you have generated a CSR (described in the previous section), you need to upload it to Microsoft Certificate server and request a CA and trusted root certificates.

➢ **To obtain Microsoft CA and trusted root certificates:**

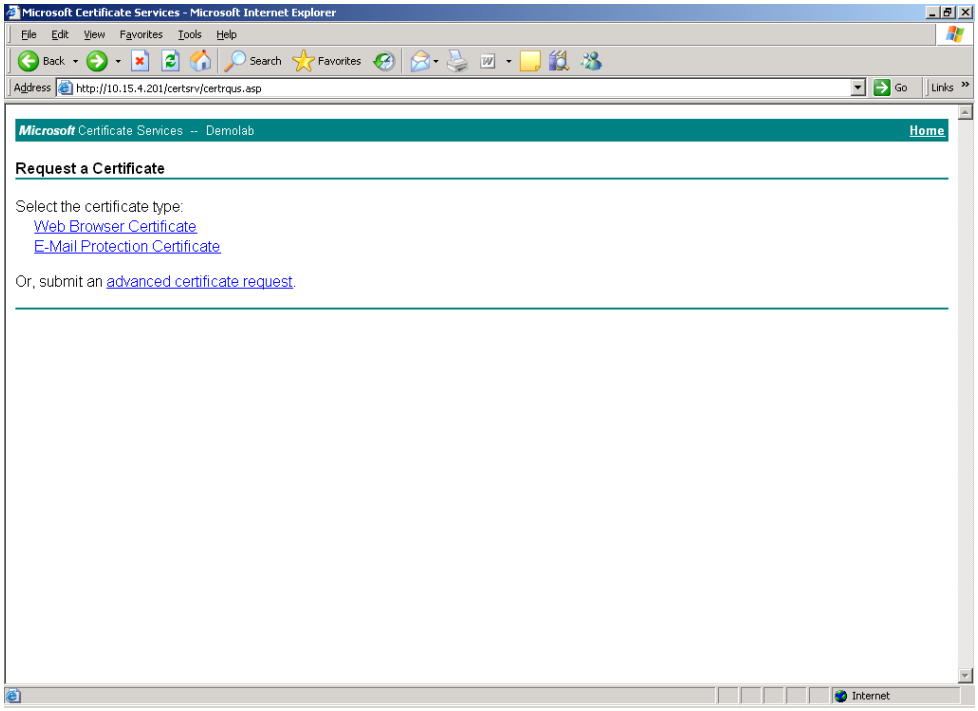
1. Open a Web browser and then navigate to Microsoft Certificate Services at **http://< certificate server address >/certsrv**.

Figure 8-11: Microsoft Certificate Services Web Page



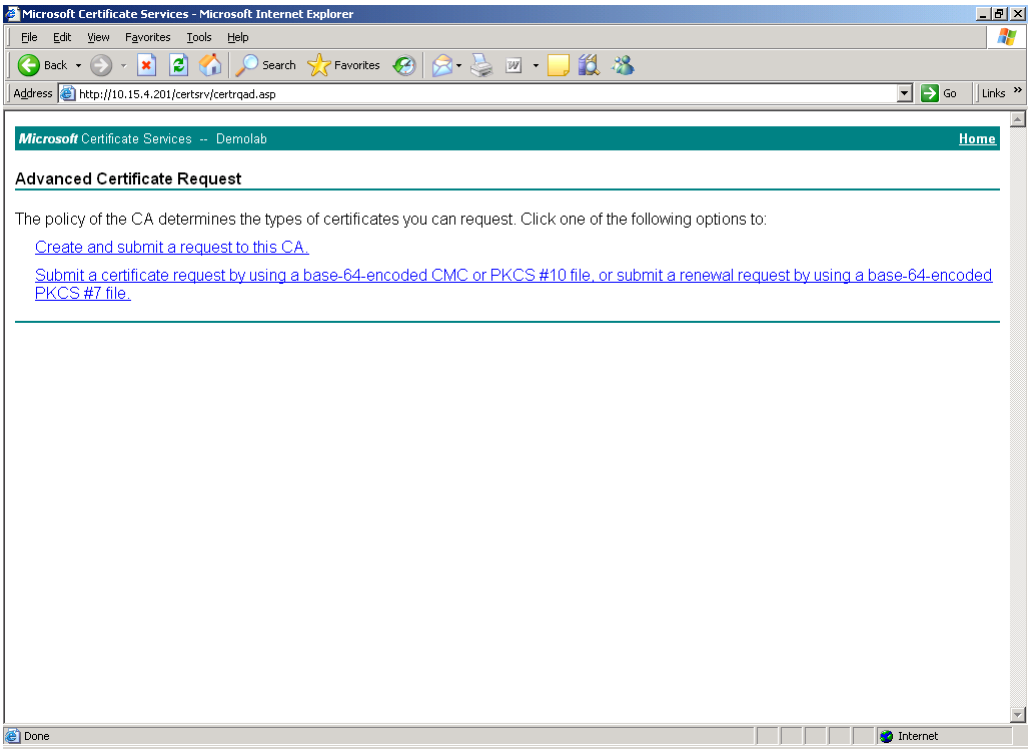
2. Click the **Request a certificate** link; the Request a Certificate page appears:

Figure 8-12: Request a Certificate Page



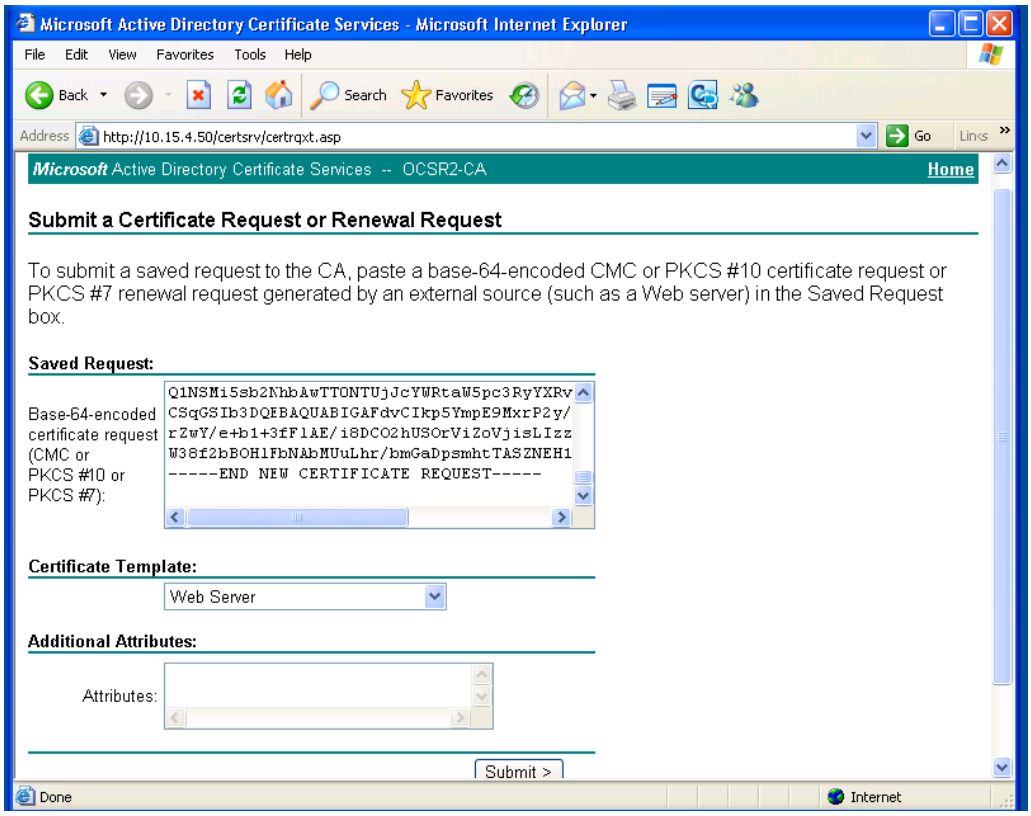
3. Click the **advanced certificate request** link; the Advanced Certificate Request page appears:

Figure 8-13: Advanced Certificate Request Page



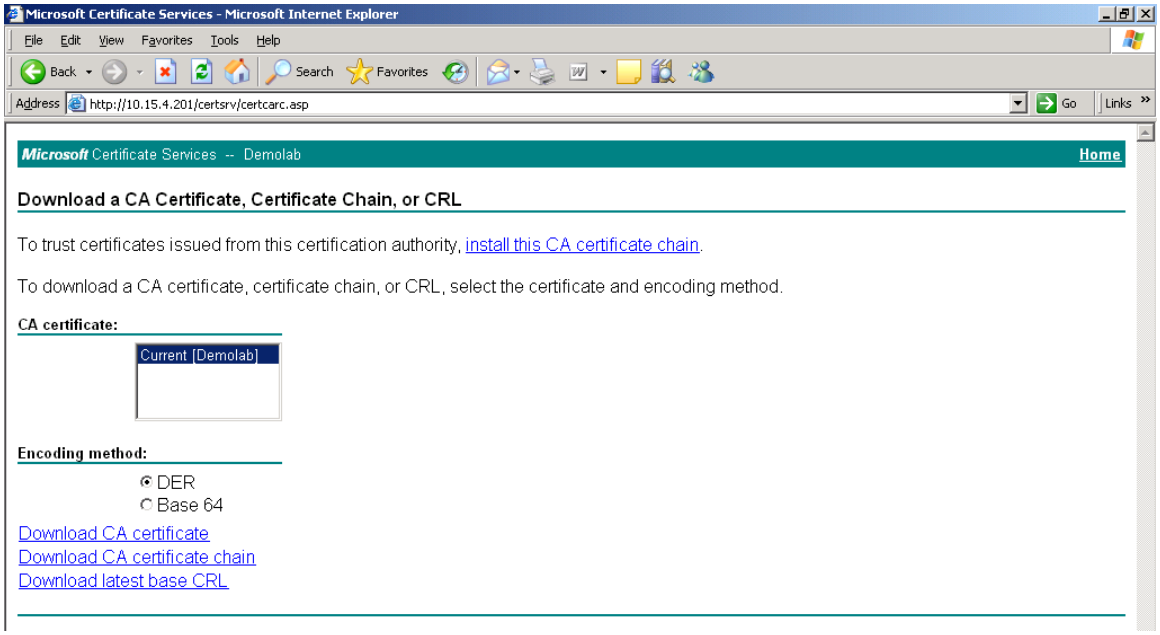
4. Click the **Submit a Certificate request by using base-64-encoded...** link; the Submit a Certificate Request or Renewal Request page appears:

Figure 8-14: Submit a Certificate Request or Renewal Request Page



5. Open the CSR file (*certreq.txt*) that you created and saved in Section 8.3.1.5.1 on page 110, and then copy its contents to the **Saved Request** text box.
6. From the **Certificate Template** drop-down list, select **Web Server**.
7. Click **Submit**.
8. Select the **Base 64** encoding option.
9. Click the **Download CA certificate** link, and then save the file with the name, *gateway.cer* in a folder on your PC.
10. Navigate once again to the certificate server at **http://< certificate server address >/certsrv**.
11. Click the **Download a CA certificate**, **certificate chain or CRL** link; the Download a CA Certificate, Certificate Chain, or CRL page appears:

Figure 8-15: Download a CA Certificate, Certificate Chain, or CRL Page



12. Under the **Encoding method** group, select the **Base 64** option.
13. Click the **Download CA certificate** link, and then save the file with the name *certroot.cer* in a folder on your PC.

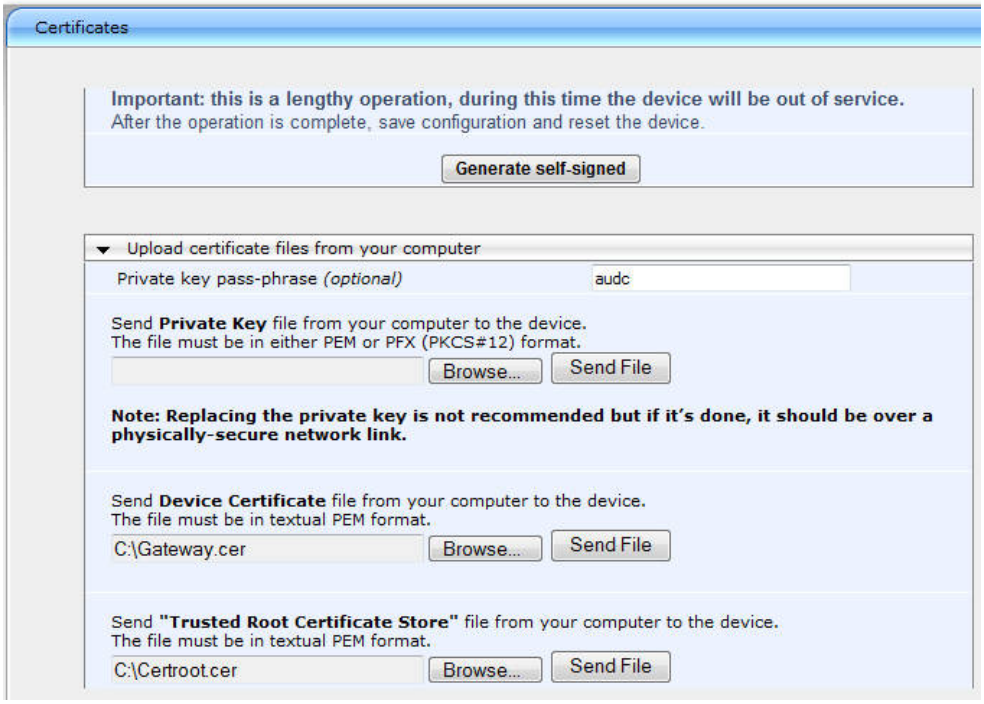
8.3.1.5.3 Load Microsoft CA and Trusted Root Certificates to PSTN Gateway

Once you have obtained the CA and trusted root certificates from Microsoft, you need to load these two certificates to the PSTN Gateway.

➢ **To load certificates to the PSTN Gateway:**

1. Open the Certificates Signing Request page (**Configuration** tab > **System** menu > **Certificates**).

Figure 8-16: Certificates Page



2. In the 'Device Certificate' field, click **Browse**, select the *gateway.cer* certificate file that you saved on your local disk (see Step 9 on page 113 in the previous section), and then click **Send File** to upload the certificate to the PSTN Gateway.
3. In the 'Trusted Root Certificate Store' field, click **Browse** to select the *certroot.cer* certificate file that you saved on your local disk (see Step 13 on page 113 in the previous section), and then click **Send File** to upload the certificate.
4. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.

8.3.2 Configuring TCP Transport Type

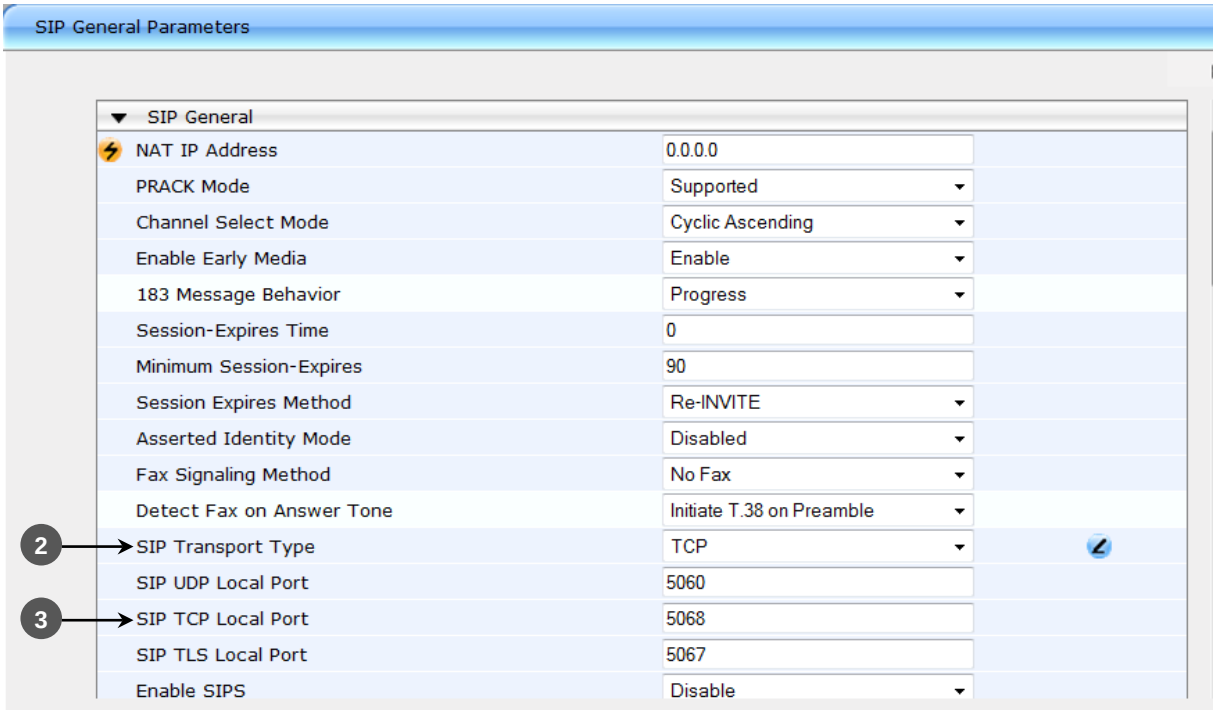
TCP provides unencrypted SIP signaling between the PSTN Gateway and Mediation Server. The procedure below describes how to configure the SIP TCP transport type.

Note: Microsoft does not recommend implementing TCP for the SIP transport type between the PSTN Gateway and the Mediation Server.

➢ **To set SIP transport type to TCP:**

1. Open the SIP General Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **General Parameters**).

Figure 8-17: SIP General Parameters Page



2. From the 'SIP Transport Type' drop-down list, select **TCP**.
3. In the 'SIP TCP Local Port' field, enter the same Gateway listening TCP port number as was configured on the Topology Builder for the gateway.
4. Click **Submit** to apply your changes.
5. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.

8.4 Configuring Secure Real-Time Transport Protocol

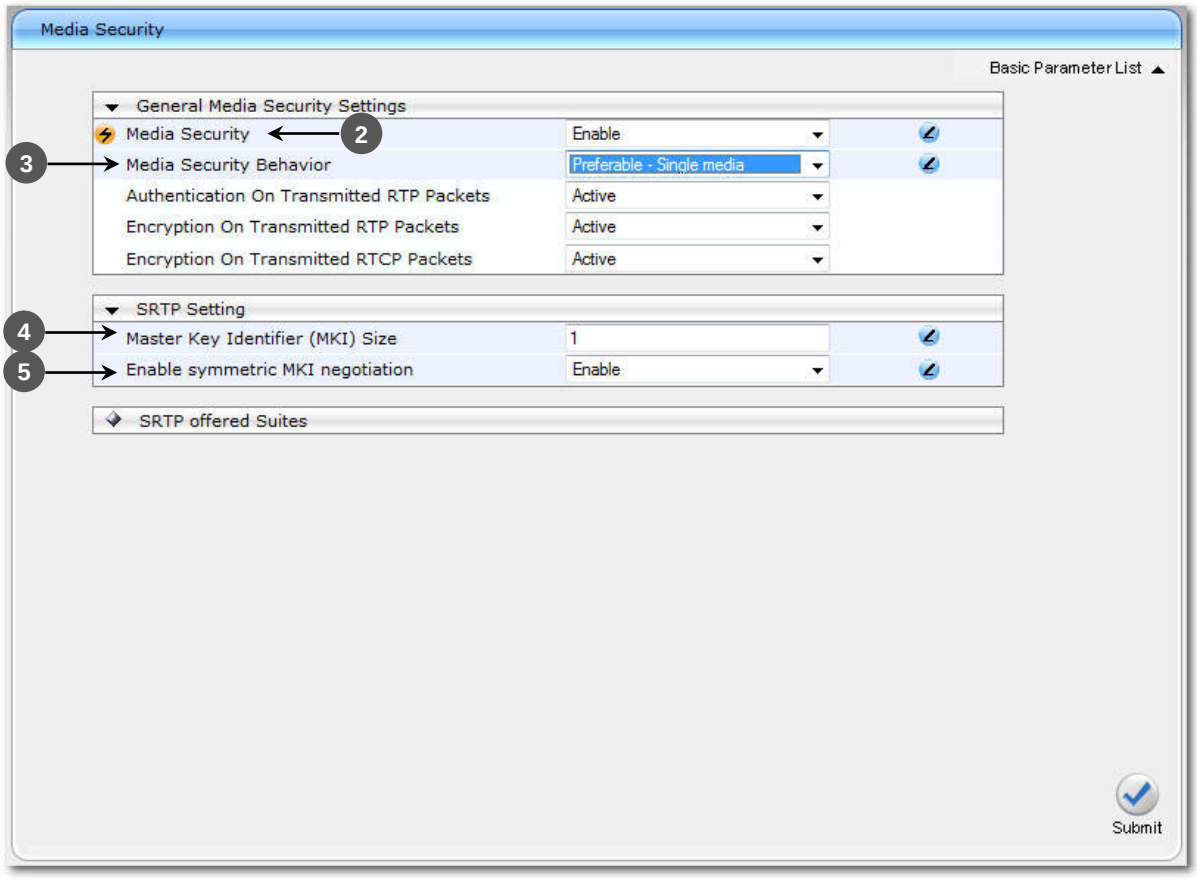
If you configure TLS as the SIP transport type between the PSTN Gateway and Mediation Server, you must enable Secure RTP (SRTP) encryption and set its mode of operation to one of the following (and that which matches the SRTP supported at the Mediation Server):

- **Preferable** (default)**:** The PSTN Gateway initiates encrypted calls. However, if negotiation of the cipher suite fails, an unencrypted call is established. Incoming calls that don't include encryption information are accepted. **This option is not supported by the Mediation server.**
- **Mandatory:** The PSTN Gateway initiates encrypted calls, but if negotiation of the cipher suite fails, the call is terminated. Incoming calls that don't include encryption information are rejected.
- **Preferable - Single Media:** The PSTN Gateway sends SDP with a single media ('m=') line only (e.g., m=audio 6000 RTP/AVP 8 0 101) with RTP/AVP and crypto keys. The remote SIP user agent (UA) can respond with SRTP or RTP parameters:
  - If the Mediation Server does not support SRTP, it uses RTP and ignores the crypto lines.
  - If the PSTN Gateway receives an SDP offer with a single media, it responds with SRTP (RTP/SAVP) if the *Media Security* parameter is set to 'Enable'. If SRTP is not supported (i.e., 'Media Security' is set to 'Disabled'), it responds with RTP.

➢ **To configure SRTP:**

1. Open the Media Security page (**Configuration** tab > **VoIP** menu > **Media** > **Media Security**).

Figure 8-18: Media Security Page



2. From the 'Media Security' drop-down list, select **Enable** to enable SRTP.

3. From the 'Media Security Behavior' drop-down list, select one of the following:
   - **Mandatory:** To force Media Security, usually used when the Mediation Server is configured to Encryption "Required".
   - **Preferable-Single media:** To prefer Media Security but support RTP as well, usually used when the Mediation Server is configured to Encryption "Optional".
4. In the 'Master Key Identifier (MKI) Size' field, enter "1". This configures the size (in bytes) of the MKI in SRTP Tx packets.
5. From the 'Enable Symmetric MKI Negotiation' drop-down list, select **Enable**.
6. Click **Submit** to apply your changes.
7. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.
8. On the toolbar, from the **Device Actions** drop-down list, choose **Reset**, and then in the' Maintenance Actions' page, click the **Reset** button; the Mediant 1000B resets and your settings are saved to the flash memory.

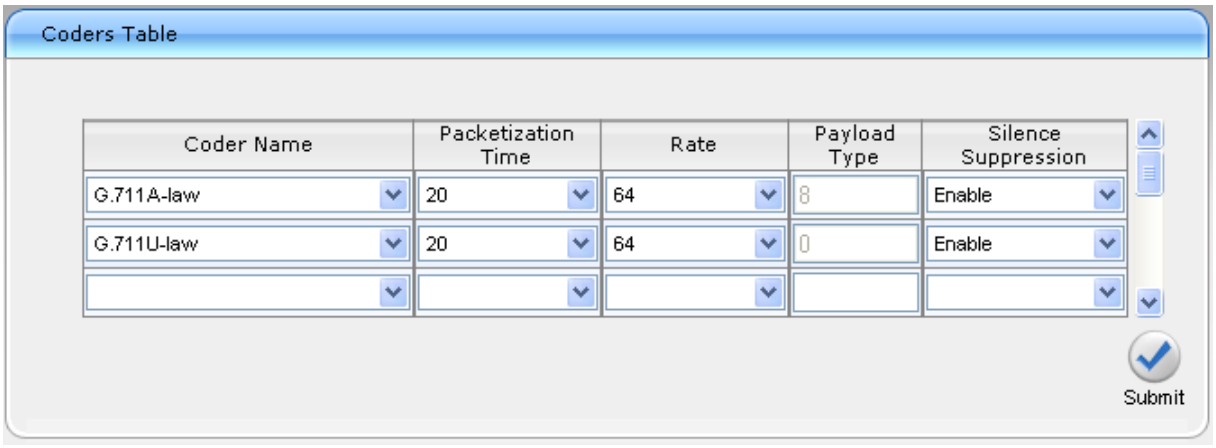
8.5 Configuring Voice Coders (with Silence Suppression)

The PSTN Gateway communicates with the Mediation Server using either the G.711 A-law or G.711 μ-law (Mu-Law) voice coder. In addition, silence suppression can be enabled per coder, which is recommended for improving the performance of the Mediation Server. The procedure below shows how you can change the default coder.

➢ **To configure the voice coder and silence suppression:**

1. Open the Coders page (**Configuration** tab > **VoIP** menu > **Coders And Profiles** > **Coders**).

Figure 8-19: Coders Table Page



2. From the 'Coder Name' drop-down list, select the required coder.
3. From the 'Silence Suppression' drop-down list, select **Enable**.
4. Click **Submit**.
5. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.

8.6 Configuring Comfort Noise and Gain Control

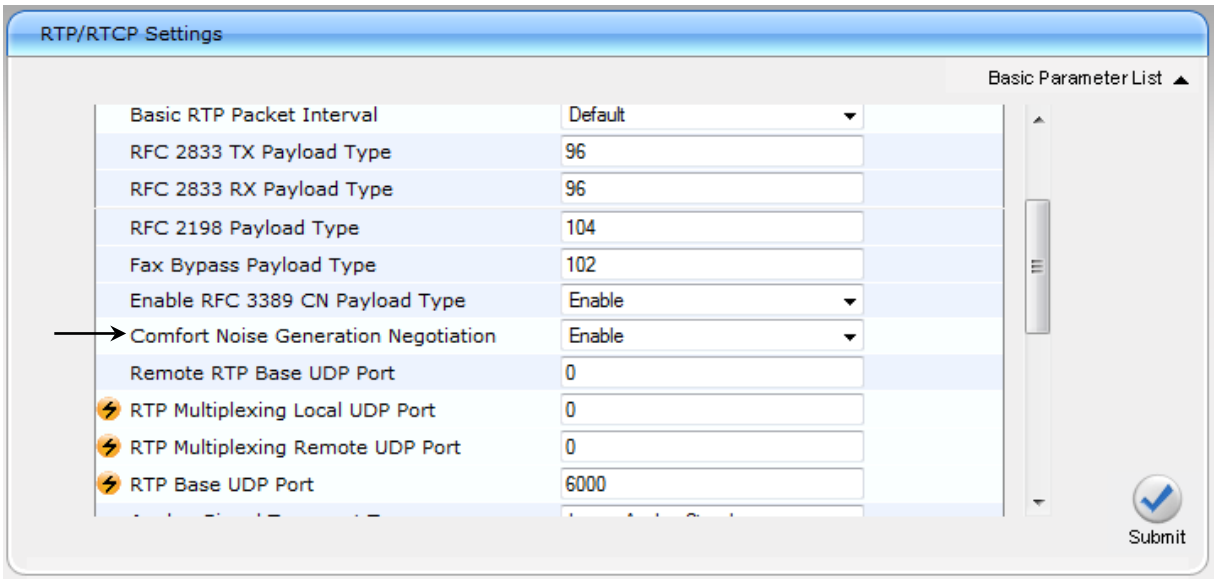
The Lync network provides high voice quality by implementing suppression of typing noise during calls and improved generation of "comfort noise," which reduces hissing and smoothes over the discontinuous flow of audio packets. You may need to configure the PSTN Gateway to match these voice quality features, by enabling silence suppression, comfort noise generation, automatic gain control (AGC), and echo canceller (enabled by default).

Note: Silence suppression is configured per coder type, as described in Section 8.5 on page 118.

➢ **To configure voice quality:**

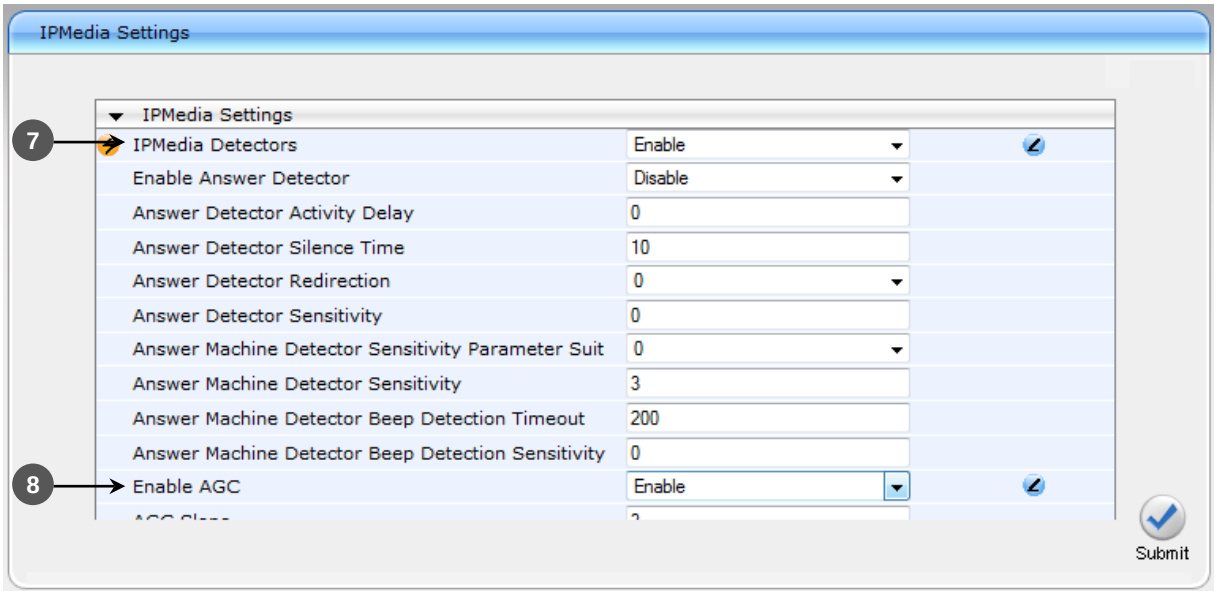
1. Open the RTP/RTCP Settings page (**Configuration** tab > **VoIP** menu > **Media** > **RTP/RTCP Settings**).

Figure 8-20: RTP/RTCP Settings Page



2. From the 'Comfort Noise Generation Negotiation' drop-down list, set **Enable** to enable comfort noise generation.
3. From the 'Enable RFC 3389 CN payload Type' drop-down list, verify **Enable**
4. Click **Submit**.
5. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.
6. Open the 'IPMedia Settings' page (**Configuration** tab > **VoIP** menu > **Media** > **IPMedia Settings**).

Figure 8-21: IPMedia Settings Page



7. From the 'IPMedia Detectors' drop-down list, select **Enable**. This parameter requires a PSTN Gateway reset (see Step 8 below).
8. From the 'Enable AGC' drop-down list, select **Enable**.
9. Click **Submit** to apply your changes.
10. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.
11. On the toolbar, from the **Device Actions** drop-down list, choose **Reset**, and then in the 'Maintenance Actions' page, click the **Reset** button; the Mediant 1000B resets and your settings are saved to the flash memory.

8.7 Configuring Early Media

Early media refers to audio and video that is exchanged before a call is accepted by the recipient. Early media generated by the caller includes voice commands or dual-tone multi frequency (DTMF) tones to activate interactive voice response (IVR) systems. Early media generated by the call recipient include ringback tones, announcements, and requests for input.

Enhanced early media support in Lync 2013 enables a caller to hear a ringback tone generated by the call recipient's mobile phone. This is also the case in team-call scenarios, where a call is routed to two team members, one of whom has configured simultaneous ringing for his or her mobile phone.

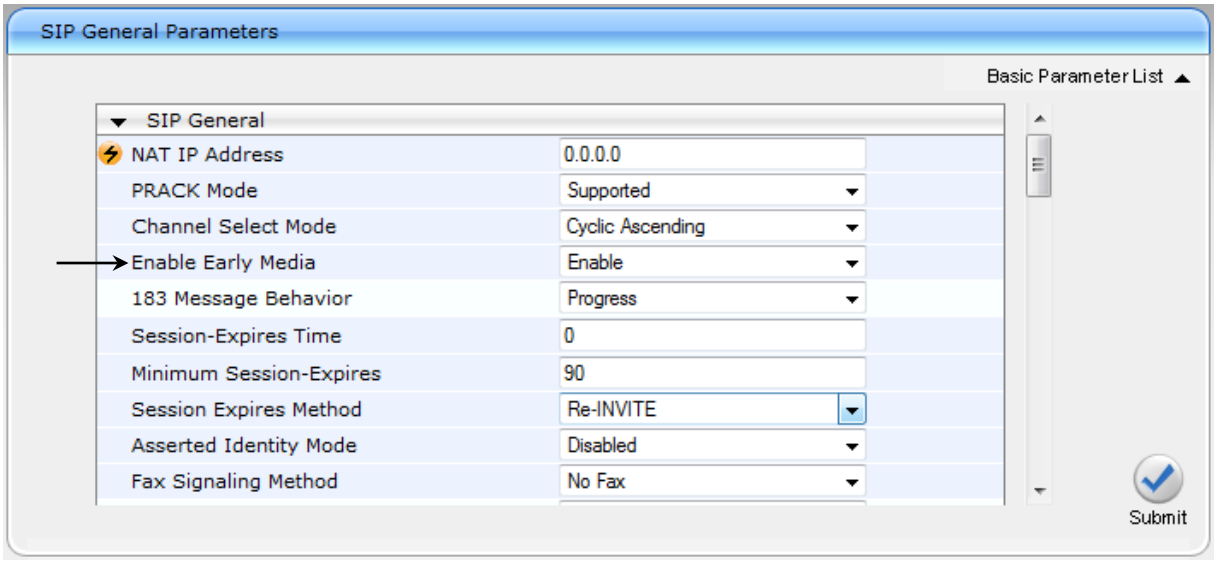
According to Lync 2013 requirements, AudioCodes PSTN Gateway must send a SIP 183 with SDP immediately after it receives an INVITE. The RTP packets however, will not be sent until the PSTN Gateway receives an ISDN Progress, Alerting and Progress Indicator or Connect message. For example, if the PSTN Gateway receives ISDN Progress, it starts sending RTP packets according to initial negotiation, but there is no need to re-send the 183 response.

You may need to configure the PSTN Gateway's early media feature to support Lync 2013 enhanced early media feature.

➢ **To configure the Early Media feature:**

1. Open the SIP General Parameters page (**Configuration** tab > **VoIP** > **SIP Definitions** > **General Parameters**).

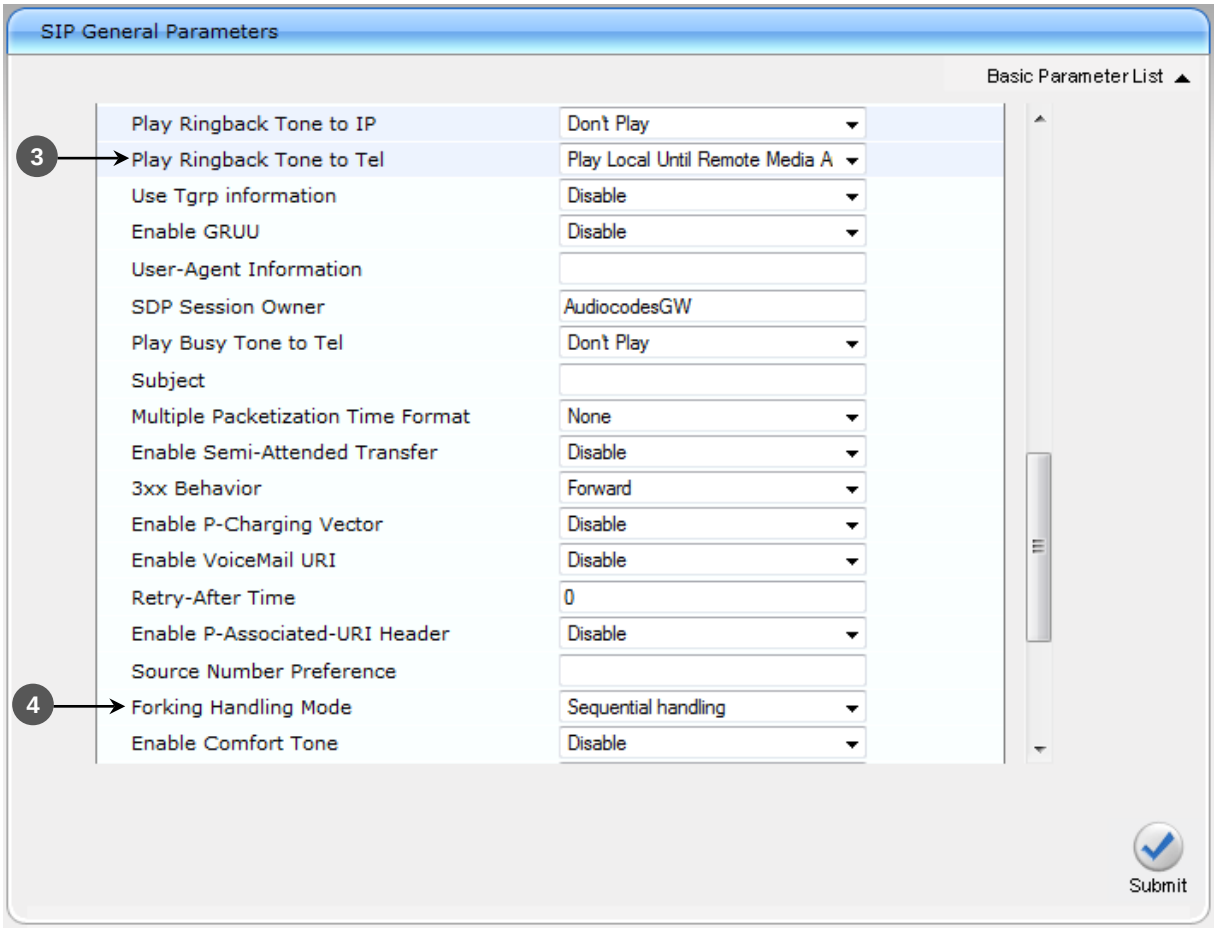
Figure 8-22: SIP General Parameters Page (1)



2. From the 'Enable Early Media' drop-down list, select **Enable**.
3. From the 'Play Ringback Tone to Tel' drop-down list, select **Play Local Until Remote Media Arrive**. If a SIP 180 response is received and the voice channel is already open (due to a previous 183 early media response or due to an SDP in the current 180 response), the PSTN Gateway plays a local ringback tone if there are no prior received RTP packets. The PSTN Gateway stops playing the local ringback tone as soon as it starts receiving RTP packets. At this stage, if the PSTN Gateway receives additional 18x responses, it does not resume playing the local ringback tone.

4. From the 'Forking Handling Mode' drop-down list, select **Sequential handling**. The PSTN Gateway opens a voice stream toward the first 18x SIP response that includes an SDP and disregards any 18x response with an SDP received thereafter.

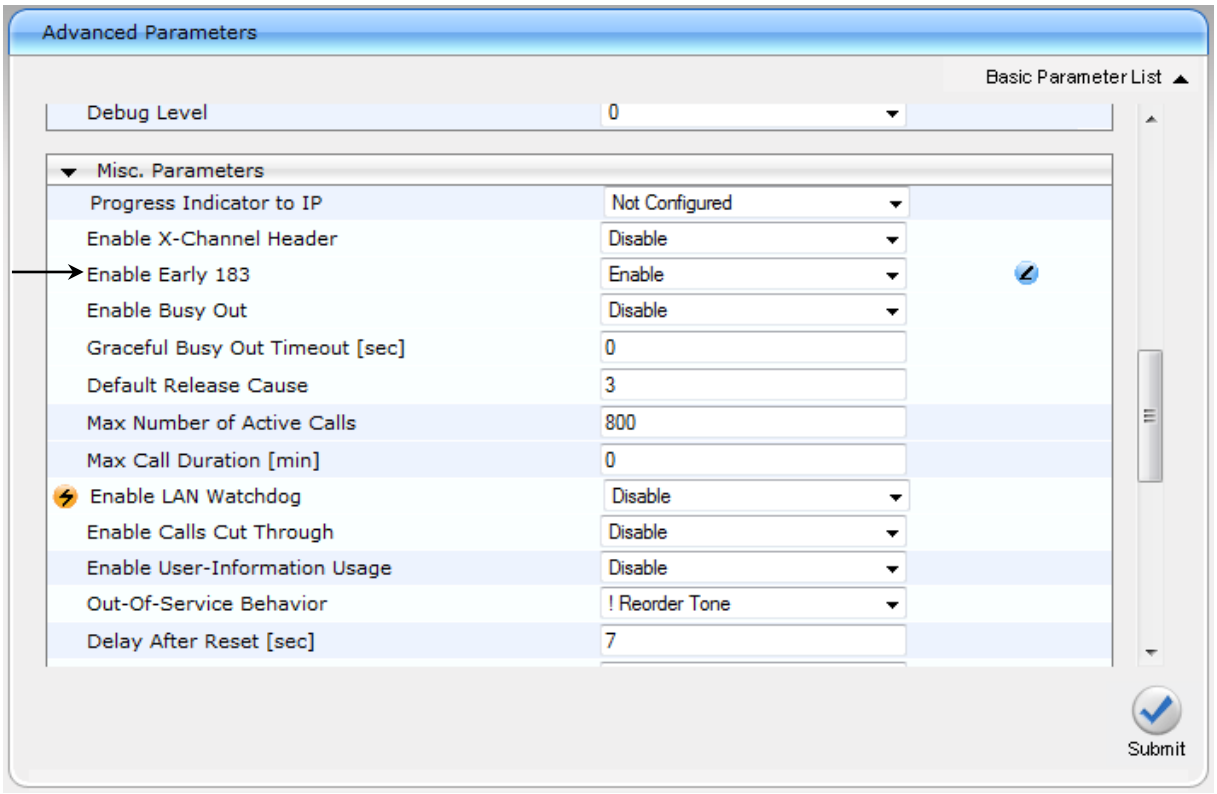
Figure 8-23: SIP General Parameters Page (2)



5. Click **Submit** to apply your changes.

6. Open the Advanced Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Advanced Parameters**).

Figure 8-24: Advanced Parameters Page



7. From the 'Enable Early 183' drop-down list, select **Enable**.
8. Click **Submit** to apply your changes.
9. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.

8.8 Configuring FXS Ports and PSTN Trunks

This section describes how to configure FXS ports and PRI (i.e., E1/T1) or BRI trunks connected to the PSTN Gateway.

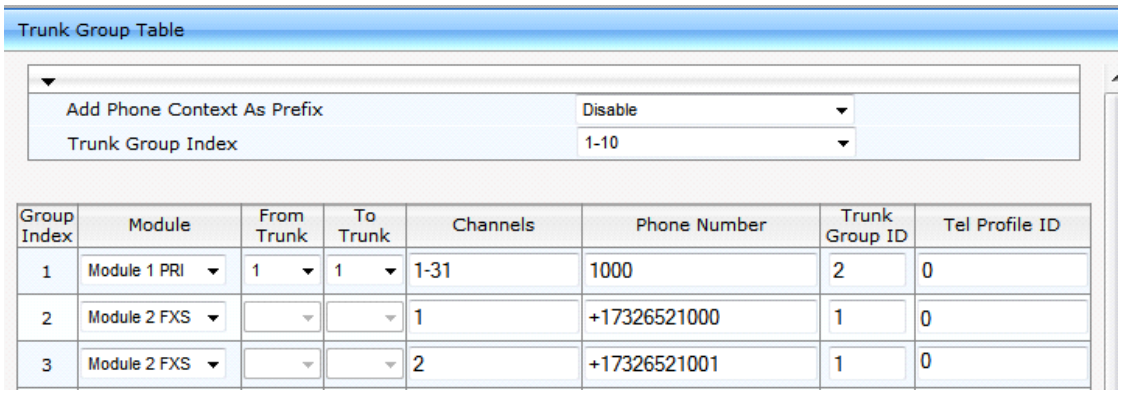
8.8.1 Enabling FXS Ports and PSTN Trunks

The procedure below describes how to enable the FXS ports and PSTN trunk (E1/T1) channels of the Enhanced gateway. This is done by defining telephone numbers for the channels and assigning them to Trunk Groups. To ensure correct routing of IP-to-Tel calls, you need to define different Trunk Groups for the digital trunk and the FXS module.

➢ **To enable the FXS ports and PSTN trunks:**

1. Open the Trunk Group Table page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Trunk Group** > **Trunk Group**).

Figure 8-25: Trunk Group Table Page



2. Define the following Trunk Groups:
   - **Trunk Group #2:** PRI module (E1/T1) with one span (1-31 channels)
   - **Trunk Group #1:** FXS module with two FXS channels – Channel 1 with phone number +17326521000 and Channel 2 with phone number +17326521001

     Those numbers need to be configured as TelUri numbers for analog devices in Lync environment using the powershell command *New-CsAnalogDevice*.
3. Click **Submit** to apply your settings.
4. On the toolbar, click **Burn** to save the changes to the Enhanced gateway flash memory.

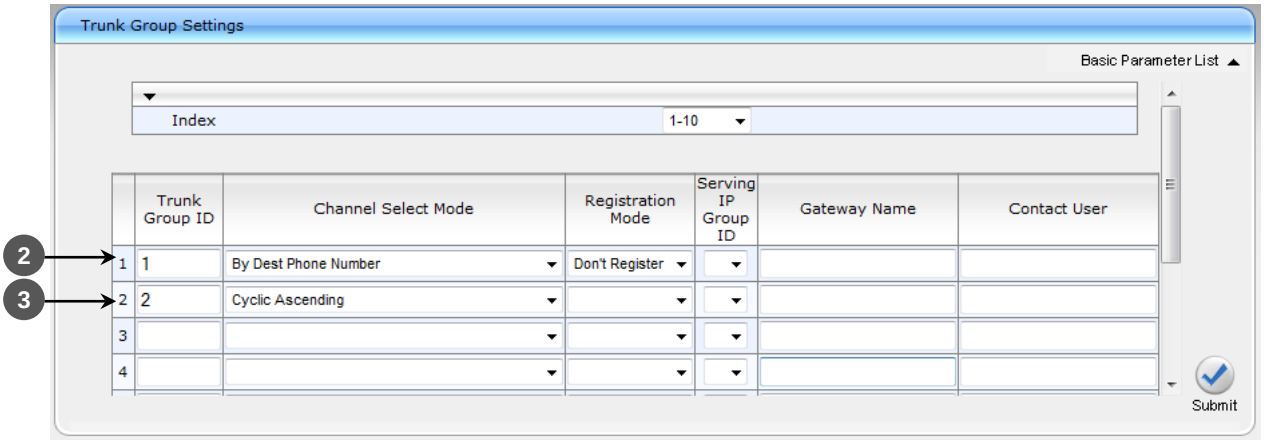
8.8.1.1 Configuring the Channel Select Method

Once you have enabled the PSTN trunk and FXS ports, and assigned them to Trunk Groups, you need to configure the method for which IP-to-Tel calls are assigned to channels within each Trunk Group.

➢ **To configure the channel select method for each Trunk Group:**

1. Open the Trunk Group Settings page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Trunk Group** > **Trunk Group Settings**).

Figure 8-26: Trunk Group Setting Page



2. For the FXS ports (i.e., Trunk Group #1), from the 'Channel Select Mode' drop-down list, select **By Dest Phone Number**. This setting sends the call to a specific FXS user according to the called (destination) number.
3. For the PSTN trunk (i.e., Trunk Group #2), from the 'Channel Select Mode' drop-down select **Cyclic Ascending**. This setting sends the call to the next available channel, in ascending cyclic order.
4. Click **Submit** to apply your settings.
5. On the toolbar, click **Burn** to save the changes to the Enhanced gateway flash memory.

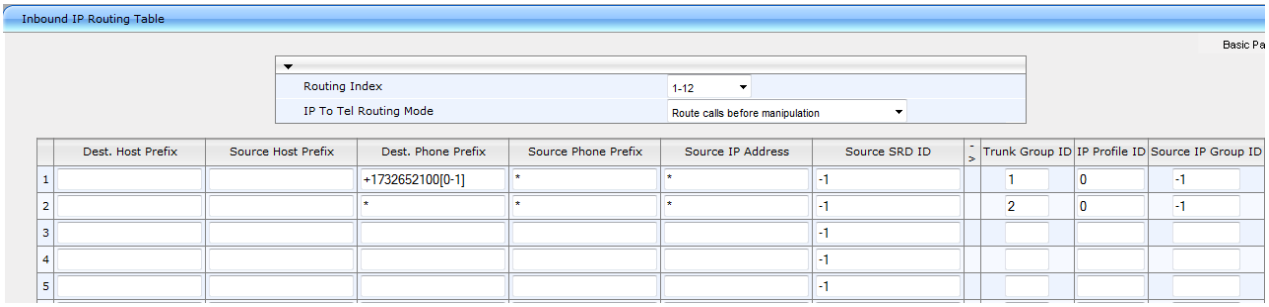
8.8.2 Configuring IP-to-Trunk Group Routing

The procedure below describes how to configure an IP-to-Trunk Group routing rule, whereby all calls to +17326521000 and +17326521001 from the Mediation Server need to be route to Trunk Group 1 (the internal FXS ports) all other calls from Mediation server need to be route to Trunk Group 2 (the PRI trunk)

➢ **To configure an IP-to-Trunk Group routing rule:**

1. Open the Inbound IP Routing Table page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Routing** > **IP to Trunk Group Routing**).

Figure 8-27: Inbound IP Routing Table Page



2. In the first table entry row, enter the +1732652100[0-1] in the 'Dest. Phone Prefix'.
3. In the 'Trunk Group ID' field, enter the Trunk Group to where the calls must be routed (Trunk Group ID 1).
4. In the second table entry row, enter asterisk sign (*) in the 'Dest. Phone Prefix'.
5. In the 'Trunk Group ID' field, enter the Trunk Group to where the calls must be routed (Trunk Group ID 2).
6. Click **Submit** to apply your changes.
7. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.

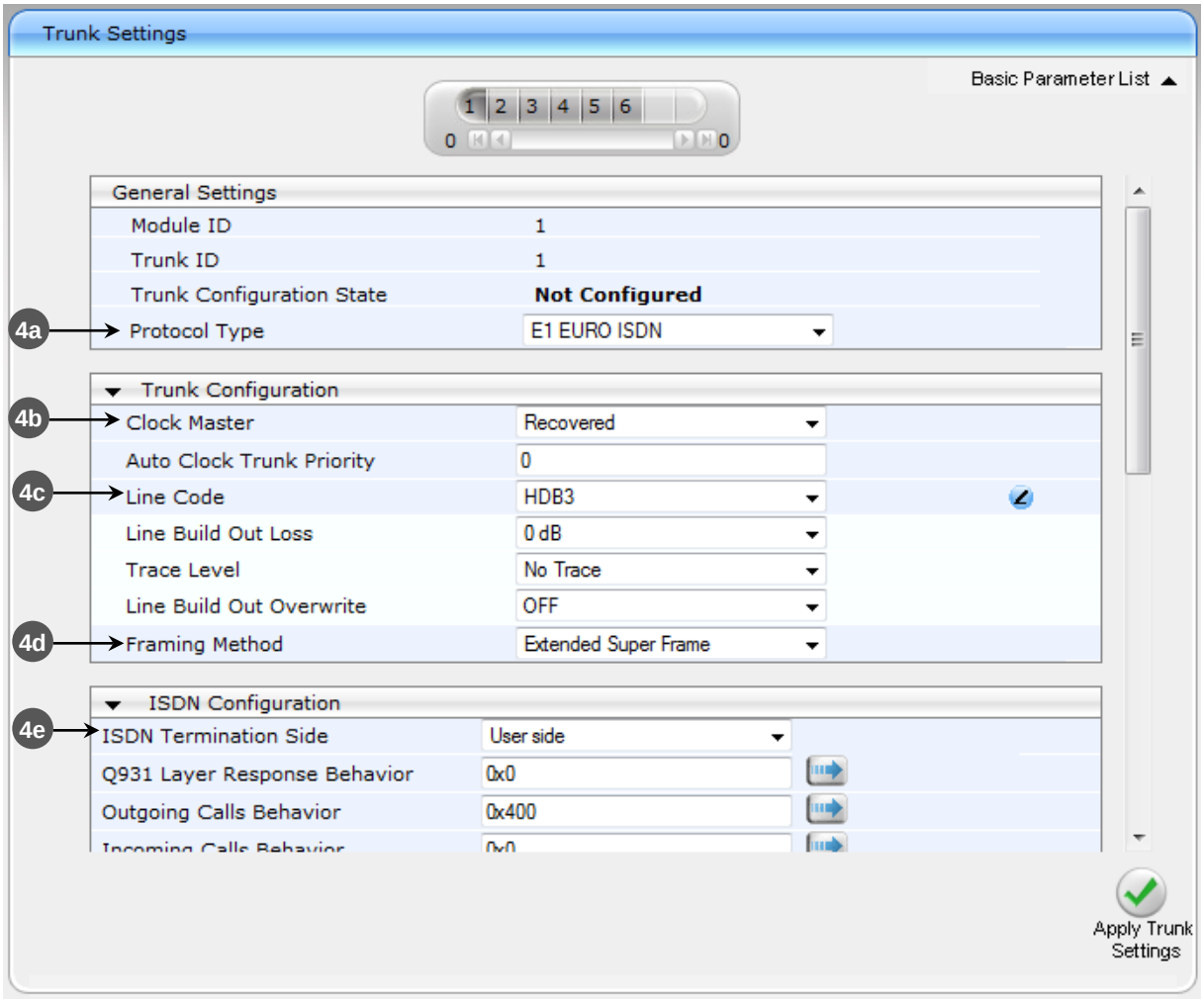
8.8.3 Configuring the Trunk

The procedure below describes basic configuration of the physical trunk.

➢ **To configure the physical trunk:**

1. Open the Trunk Settings page (**Configuration** tab > **VoIP** menu > **PSTN** > **Trunk Settings**).

Figure 8-28: Trunk Settings Page



2. On the top of the page, a bar with trunk number icons displays the status of each trunk:
   - Grey - disabled
   - Green - active
   - Yellow - RAI alarm
   - Red - LOS / LOF alarm
   - Blue - AIS alarm
   - Orange - D-channel alarm (ISDN only)

   Select the Trunk that you want to configure, by clicking the desired trunk number icon.
3. If the trunk is new, configure the trunk as required. If the trunk was previously configured, click the **Stop Trunk** button to de-activate the trunk.

4. Basic trunk configuration:
   a. From the 'Protocol Type' drop-down list, select the required trunk protocol.

Note:

- If the 'Protocol Type' field displays 'NONE' (i.e., no protocol type selected) and no other trunks have been configured, after selecting a PRI protocol type, you must reset the PSTN Gateway.
- All PRI trunks of the PSTN Gateway must be of the same line type - E1 or T1. However, different variants of the same line type can be configured on different trunks, for example, E1 Euro ISDN and E1 CAS (subject to the constraints in the Release Notes).
- BRI trunks can operate with E1 or T1 trunks.
- If the trunk can't be stopped because it provides the clock (assuming the PSTN Gateway is synchronized with the E1/T1 clock), assign a different E1/T1 trunk to provide the clock or enable 'TDM Bus PSTN Auto Clock' in the 'TDM Bus Settings' page (see Section 8.8.4 on page 129).
- To delete a previously configured trunk, set the *Protocol Type* parameter to 'None'.

   b. From the 'Clock Master' drop-down list, select the trunk's clock source:
      - **Recovered:** Clock source is recovered from the trunk
      - **Generated:** Clock source is provided by the internal TDM bus clock source (according to the *TDM Bus Clock Source* parameter – see Section 8.8.4 on page 129)
   c. From the 'Line Code' drop-down list, select the line code:
      - **B8ZS:** (bipolar 8-zero substitution) for T1 trunks only
      - **HDB3:** (high-density bipolar 3) for E1 trunks only
      - **AMI:** (for E1 and T1)
   d. From the 'Framing Method' drop-down list, select the required framing method. For E1 trunks always select **Extended Super Frame**.
   e. To configure whether the trunk connected to the PBX is User or Network side for QSIG, from the 'ISDN Termination' drop-down list, select **User side** or **Network side**.
5. Continue configuring the trunk according to your requirements.
6. When you have completed configuration, click the **Apply Trunk Settings** button to apply the changes to the selected trunk.
7. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.

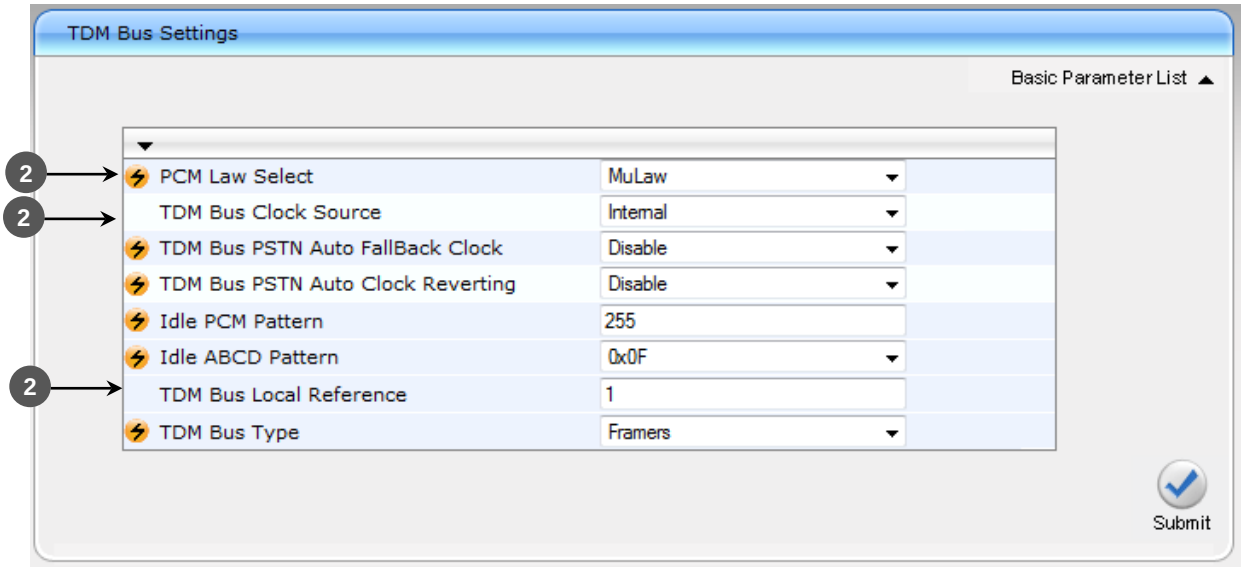
8.8.4 Configuring the TDM Bus

The procedure below describes how to configure the TDM bus of the PSTN Gateway.

➢ **To configure the TDM bus:**

1. Open the TDM Bus Settings page (**Configuration** tab > **VoIP** menu > **TDM** > **TDM Bus Settings**).

Figure 8-29: TDM Bus Settings Page



2. Configure the TDM bus parameters according to your deployment requirements. Below is a description of some of the main TDM parameters:
   - **PCM Law Select:** defines the type of PCM companding law in the input/output TDM bus. Typically, A-Law is used for E1 and Mu-Law for T1/J1.
   - **TDM Bus Clock Source:** defines the clock source to which the PSTN Gateway synchronizes - generate clock from local source (Internal) or recover clock from PSTN line (Network).
   - **TDM Bus Local Reference:** defines the physical trunk ID from which the PSTN Gateway recovers (receives) its clock synchronization when the TDM Bus Clock Source is configured to recover the clock from the PSTN line.
3. Click **Submit** to apply your changes.
4. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.
5. On the toolbar, from the **Device Actions** drop-down list, choose **Reset**, and then in the 'Maintenance Actions' page, click the **Reset** button; the Mediant 1000B resets and your settings are saved to the flash memory.

8.9 Configuring Normalization Rules for E.164 Format for PBX/PSTN Connectivity

Lync 2013 implements the standard E.164 format, while the PBX or PSTN implements other number formats for dialing. If the PSTN Gateway is connected to a PBX or directly to the PSTN, the PSTN Gateway may need to perform number manipulations for the called and/or calling number to match the PBX or PSTN dialing rules or to match Lync 2013 E.164 format.

Therefore, the PSTN Gateway must be configured with manipulation rules to translate (i.e., normalize) numbers dialed in standard E.164 format to various formats, and vice versa. Manipulation needs to be done for outbound calls (i.e., calls received from Lync clients through Lync 2013) and inbound calls (i.e., calls destined to Lync clients).

Number manipulation (and mapping of NPI/TON to SIP messages) rules are configured in the following Manipulation tables:

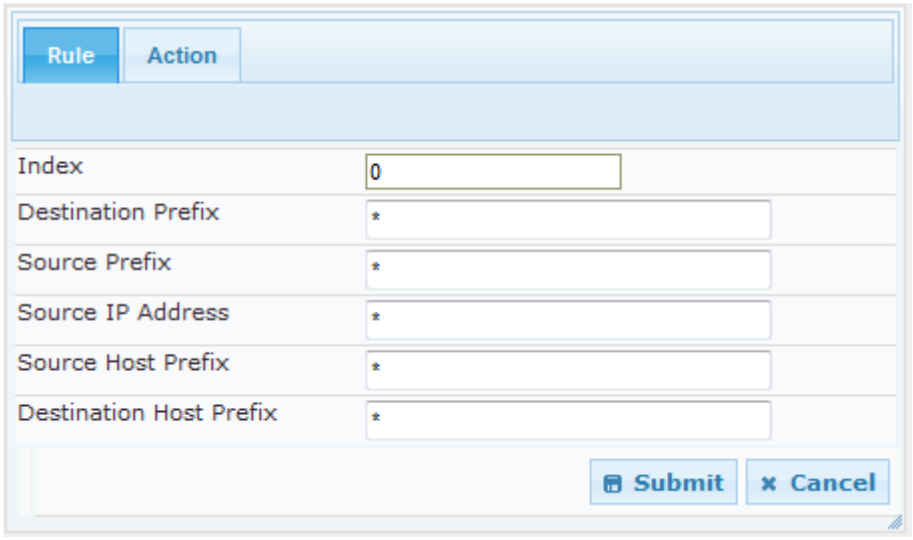
- **For Tel-to-IP calls:**
  - Destination Phone Number Manipulation Table for Tel-to-IP Calls
  - Source Phone Number Manipulation Table for Tel-to-IP Calls
- **For IP-to-Tel calls:**
  - Destination Phone Number Manipulation Table for IP-to-Tel Calls
  - Source Phone Number Manipulation Table for IP-to-Tel Calls

Number manipulation configuration examples are provided for inbound and outbound calls in Section 8.9.1 on page 134.

➢ **To configure number manipulation rules:**

1. Open the required number Manipulation table (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Manipulations**); the relevant Manipulation table page is displayed
2. Click the **Add** button; the following dialog box appears:

Figure 8-30: Number Manipulation Table - Add Dialog Box



3. Click the **Rule** tab, and then configure the matching characteristics. For a description of the parameters, see the table below.
4. Click the **Action** tab, and then configure the manipulation operation. For a description of the parameters, see the table below.
5. Configure manipulation rules as required.

6. Click **Submit** to apply your changes.
7. On the toolbar, click **Burn** to save the settings to the PSTN Gateway; the PSTN Gateway resets, saving the settings to flash memory.

Table 8-1: Number Manipulation Parameters Description

Parameter	Description
Matching Characteristics (Rule)	
Destination Prefix	Defines the destination (called) telephone number prefix and/or suffix. You can use special notations for denoting the prefix. For example, **[100-**199](100,101,105) denotes a number that starts with 100 to 199 and ends with 100, 101 or 105. You can also use the $ sign to denote calls without a called number.
Source Prefix	Defines the source (calling) telephone number prefix and/or suffix. You can use special notations for denoting the prefix. For example, **[100-**199](100,101,105) denotes a number that starts with 100 to 199 and ends with 100, 101 or 105. You can also use the $ sign to denote calls without a calling number.
Source IP Address	Defines the source IP address of the caller. This is obtained from the Contact header in the INVITE message. **Notes:** ▪ This parameter is applicable only to the number manipulation tables for IP-to-Tel calls. ▪ The source IP address can include the 'x' wildcard to represent single digits. For example: 10.8.8.xx represents all IP addresses between 10.8.8.10 to 10.8.8.99. ▪ The source IP address can include the asterisk (*) wildcard to represent any number between 0 and 255. For example, 10.8.8.* represents all IP addresses between 10.8.8.0 and 10.8.8.255.
Source Host Prefix	Defines the URI host name prefix of the incoming SIP INVITE message in the From header. **Notes:** ▪ This parameter is applicable only to the number manipulation tables for IP-to-Tel calls. ▪ The asterisk (*) wildcard can be used to denote any prefix. ▪ If the P-Asserted-Identity header is present in the incoming INVITE message, then the value of this parameter is compared to the P-Asserted-Identity URI host name (instead of the From header).
Destination Host Prefix	Defines the Request-URI host name prefix of the incoming SIP INVITE message. **Notes:** ▪ This parameter is applicable only to the number manipulation tables for IP-to-Tel calls. ▪ The asterisk (*) wildcard can be used to denote any prefix.

Parameter	Description
Source Trunk Group	Defines the source Trunk Group ID for Tel-to-IP calls. To denote all Trunk Groups, leave this field empty. **Notes:** ▪ The value -1 indicates that this field is ignored in the rule. ▪ This parameter is applicable only to the number manipulation tables for Tel-to-IP calls. ▪ For IP-to-IP call routing, this parameter is not required (i.e., leave the field empty).
Source IP Group	Defines the IP Group from where the IP call originated. Typically, the IP Group of an incoming INVITE is determined or classified using the Inbound IP Routing Table. If not used (i.e., any IP Group), leave the field empty. **Notes:** ▪ The value -1 indicates that this field is ignored. ▪ This parameter is applicable only to the number manipulation tables for Tel-to-IP calls. ▪ If this Source IP Group has a Serving IP Group, then all calls from this Source IP Group are sent to the Serving IP Group. In this scenario, this table is used only if the PreferRouteTable parameter is set to 1.
Destination IP Group	Defines the IP Group to where the call is sent. **Notes:** ▪ The value -1 indicates that this field is ignored. ▪ This parameter is applicable only to the Destination Phone Number Manipulation Table for Tel -> IP Calls.
Operation (Action)	
Stripped Digits From Left	Defines the number of digits to remove from the left of the telephone number prefix. For example, if you enter 3 and the phone number is 5551234, the new phone number is 1234.
Stripped Digits From Right	Defines the number of digits to remove from the right of the telephone number prefix. For example, if you enter 3 and the phone number is 5551234, the new phone number is 5551.
Prefix to Add	Defines the number or string that you want added to the front of the telephone number. For example, if you enter 9 and the phone number is 1234, the new number is 91234.
Suffix to Add	Defines the number or string that you want added to the end of the telephone number. For example, if you enter 00 and the phone number is 1234, the new number is 123400.
Number of Digits to Leave	Defines the number of digits that you want to keep from the right of the phone number. For example, if you enter 4 and the phone number is 00165751234, then the new number is 1234.

Parameter	Description
NPI	Defines the Numbering Plan Indicator (NPI). ▪ **[0]** Unknown (default) ▪ **[9]** Private ▪ **[1]** E.164 Public ▪ **[-1**] Not Configured = value received from PSTN/IP is used **Notes:** ▪ This parameter is applicable only to number manipulation tables for IP-to-Tel calls. ▪ NPI can be used in the SIP Remote-Party-ID header by using the *EnableRPIHeader* and *AddTON2RPI* parameters. .
TON	Defines the Type of Number (TON). ▪ If you selected 'Unknown' for the NPI, you can select Unknown **[0].** ▪ If you selected 'Private' for the NPI, you can select Unknown **[0],** Level 2 Regional **[1],** Level 1 Regional **[2],** PISN Specific **[3]** or Level 0 Regional (Local) **[4].** ▪ If you selected 'E.164 Public' for the NPI, you can select Unknown **[0],** International **[1],** National **[2],** Network Specific **[3],** Subscriber **[4]** or Abbreviated **[6].** The default is 'Unknown'. **Notes:** ▪ This parameter is applicable only to number manipulation tables for IP-to-Tel calls. ▪ TON can be used in the SIP Remote-Party-ID header by using the *EnableRPIHeader* and *AddTON2RPI* parameters. .
Presentation	Enables Caller ID. ▪ Not Configured = Privacy is determined according to the Caller ID table. ▪ **[0]** Allowed = Sends Caller ID information when a call is made using these destination/source prefixes. ▪ **[1]** Restricted = Restricts Caller ID information for these prefixes. **Notes:** ▪ This field is applicable only to number manipulation tables for source phone number manipulation. ▪ If this field is set to **Restricted** and the 'Asserted Identity Mode' (AssertedIdMode) parameter is set to **P-Asserted**, the From header in the INVITE message includes the following: From: 'anonymous' <sip: anonymous@anonymous.invalid> and 'privacy: id' header.

8.9.1 Number Normalization Examples

Two examples are provided below for number normalization. The examples are based on the following assumptions:

- PBX with prefix (local) number 333
- 4-digit extension numbers that begin with the digit 1 (i.e., 1xxx)
- National area code is 206
- Country code is 1

8.9.1.1 Modifying E.164 Numbers to PBX / PSTN Format for Outbound Calls

Outbound calls refer to calls made by Lync clients to a PBX / PSTN number.

1. **Local Calls within PBX:** The caller dials only the last four digits (e.g., 1212). Lync translates (normalizes) the phone number into an E.164 number format: +12063331212 (where *+1* is the country code, *206* the local area code, and *333* the PBX prefix number). The Manipulation table is configured to send only the last four digits to the PBX (i.e., 1212).
2. **National Calls to the Same Area Code:** The caller dials 9 for an external line, and then dials a 7-digit telephone number (e.g., 9-555-4321). Lync translates (normalizes) the phone number into an E.164 number format: +12065554321 (where *+1* is the country code, *206* the local area code, *5554321* the phone number). The Manipulation table is configured to remove (strip) the first five digits and add 9 as a prefix to the remaining number. Therefore, the PSTN Gateway sends the number 95554321 to the PBX, and then the PBX sends the number 5554321 to the PSTN.
3. **National Calls to a Different Area Code:** The caller dials 9 for an external line, the out-of-area code, and then a 7-digit telephone number (e.g., 9-503-331-1425). Lync translates (normalizes) the phone number into an E.164 number format: +15033311425 (where *+1* is the international code, *503* the out-of area code, *3311425* the phone number). The Manipulation table is configured to remove (strip) the first two digits (i.e., *+1*), add then add 9 as a prefix to the remaining number. Therefore, the PSTN Gateway sends the number 95033311425 to the PBX, and then the PBX sends the number 5033311425 to the PSTN.
4. **Dialing International Calls:** The caller dials 9 for an external line, the access code for international calls (e.g., 011 for the US), the country code (e.g., +44 for the UK), the area code (e.g., 1483), and then a 6-digit telephone number (e.g., 829827). Lync translates (normalizes) the phone number into an E.164 number format: +441483829827 (where *+44* is the country code, *1483* the area code, *829827* the phone number). The Manipulation table is configured to remove the first digit (e.g., +), and add the external line digit (e.g., 9) and the access code for international calls (e.g., 011 for the US) as the prefix. Therefore, the PSTN Gateway sends the number 9011441483829827 to the PBX and the PBX, in turn, sends the number 011441483829827 to the PSTN.

The configuration of the above scenarios is shown in Figure 8-31.

Figure 8-31: Destination Phone Number Manipulation Table for IP→Tel Calls

8.9.1.2 Modifying PBX, Local, and National Calls to E.164 Format for Inbound Calls

Inbound calls refer to calls received by Lync clients from the PBX / PSTN.

1. **Local Calls from the PBX / PSTN:** The PBX user only dials a 4-digit extension number of the Lync client (e.g., 1220). The Manipulation table is configured to normalize the number into E.164 format and adds the prefix +1206333 to the extension number. Therefore, the PSTN Gateway sends the number +12063331220 to Lync, which relays the call to the Lync client.
2. **National Calls with the Same Area Code**: The PSTN user dials a 7-digit phone number (e.g., 333-1220), which is received by the PSTN Gateway. The Manipulation table is configured to normalize the number into E.164 format and adds the prefix +1206 to the number. Therefore, the PSTN Gateway sends the number +12063331220 to Lync, which relays the call to the Lync client.
3. **National Calls from a Different Area Code:** The PSTN user dials the national area code and then a 7-digit phone number (e.g., 206-333-1220), which is received by the PSTN Gateway. The Manipulation table is configured to normalize the number into E.164 format and adds the prefix +1 to the number. Therefore, the PSTN Gateway sends the number +12063331220 to Lync, which relays the call to the Lync client.

Note: Whether the area code is received by the PSTN Gateway depends on the country's PSTN numbering rules.

4. **International Calls:** The PSTN international (overseas) caller dials the international access and country code (e.g., 001 for the US), the national area code, and then a 7-digit phone number (e.g., 206-333-1220), which is received by the PSTN Gateway. The Manipulation table is configured to normalize the number into E.164 format, by removing the first two digits (e.g., 00) and adding the prefix plus sign (+). Therefore, the PSTN Gateway sends the number +12063331220 to Lync, which relays the call to the Lync client.

Note: Whether the area code is received by the PSTN Gateway depends on the country's PSTN numbering rules.

The configuration of the above scenarios is shown in the figure below:

Figure 8-32: Destination Phone Number Manipulation Table for Tel→IP Calls

Destination Phone Number Manipulation Table for Tel -> IP Calls

Add + | Insert +

Index	Destination Prefix	Source Prefix	Source Trunk Group	Destination IP Group	Prefix to Add	Suffix to Add
1	1xxx	*	-1	-1	+1206333	
2	333	*	-1	-1	+1206	
3	206	*	-1	-1	+1	
4	00	*	-1	-1	+	

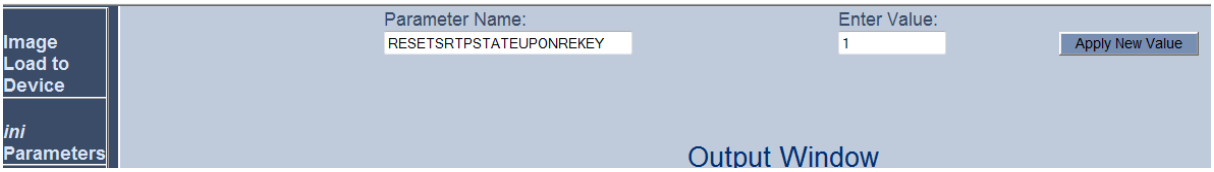
Page 1 of 1 Show 10 records per page View 1 - 4 of 4

8.10 Configuring SRTP Behavior upon Rekey Mode

➢ **To configure the SRTP behavior upon rekey mode:**

1. Open the Admin page by appending the case-sensitive suffix 'AdminPage' to the SBC's IP address in your Web browser's URL field (e.g., http://10.15.9.101/AdminPage).

Figure 8-33: AdminPage



2. In the left menu, click ***ini* Parameters**.
3. In the 'Parameter Name' field, enter "RESETSRTPSTATEUPONREKEY".
4. In the 'Enter Value' field, enter **1**.
5. Click the **Apply New Value** button.

8.11 Configuring FXS Port Transfer Behavior

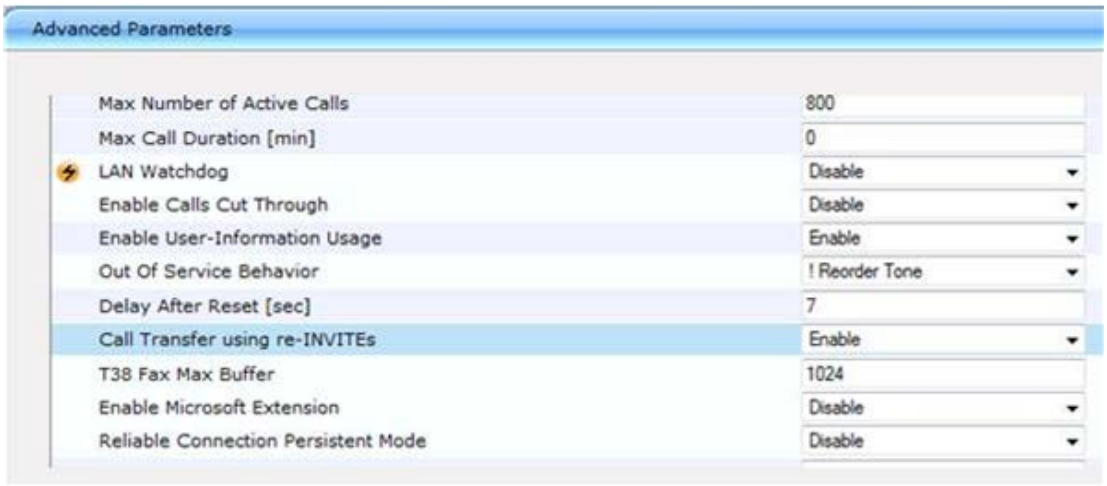
Since the Mediation server does not support receiving SIP Refer messages, you must configure the Enhanced gateway FXS port to send INVITE messages (in the event when call transfer is initiated from the FXS port).

Note: For this feature to work, an MPM module is required, and media channels should be configured according to the number of FXS ports (see below).

➢ **To configure the FXS port transfer feature using the re-invites parameter:**

1. Open the Advanced Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Advanced Parameters**).

Figure 8-34: Enable Call Transfer Using Re-invites



2. From the 'Call Transfer using re-INVITEs' drop-down list, select **Enable**.
3. Click **Submit**.

➢ **To configure media channels:**

1. Open the IP Media Settings page (**Configuration** tab > **VoIP** > **IP Media** > **IP Media Settings**).

Figure 4-29: IP Media Settings

2. In the 'Number of Media Channels' field, enter the number of media channels; two media channels for each FXS port.
3. Click **Submit**.

Reader's Notes

9 Testing SBA Calls

Once you have completed the configuration steps described in the previous sections, you can test call making at the branch office, as described in this section.

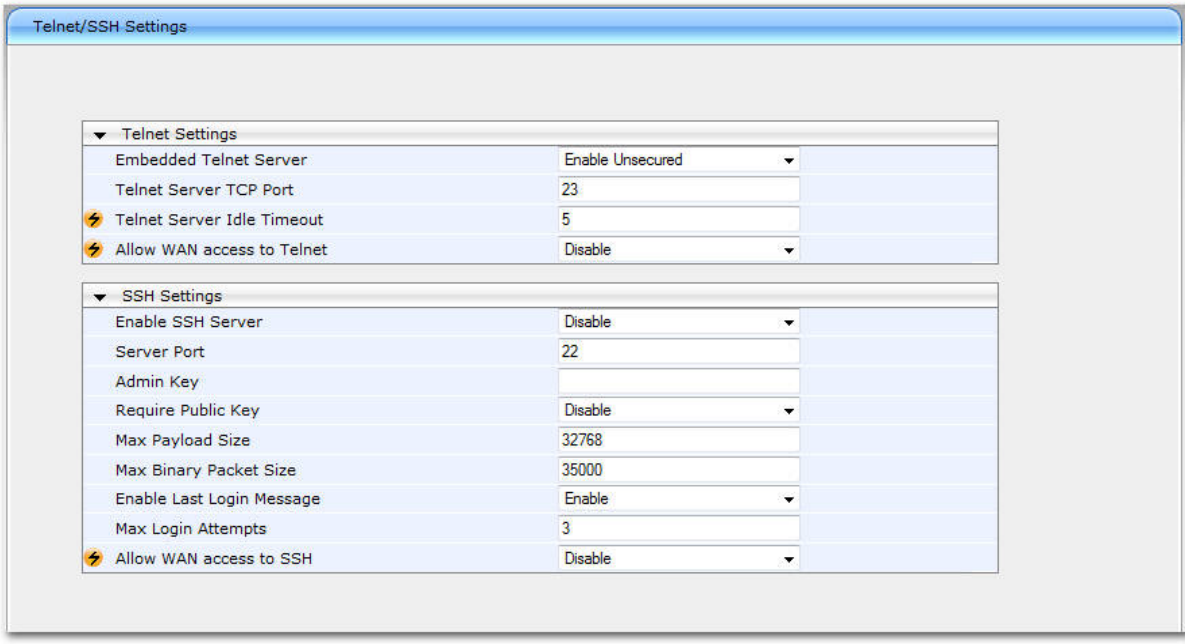
9.1 Testing Gateway Calls

The procedure below describes how to test calls on the PSTN Gateway. Before you do this, you need to establish a telnet session with the PSTN Gateway.

➢ **To test gateway calls:**

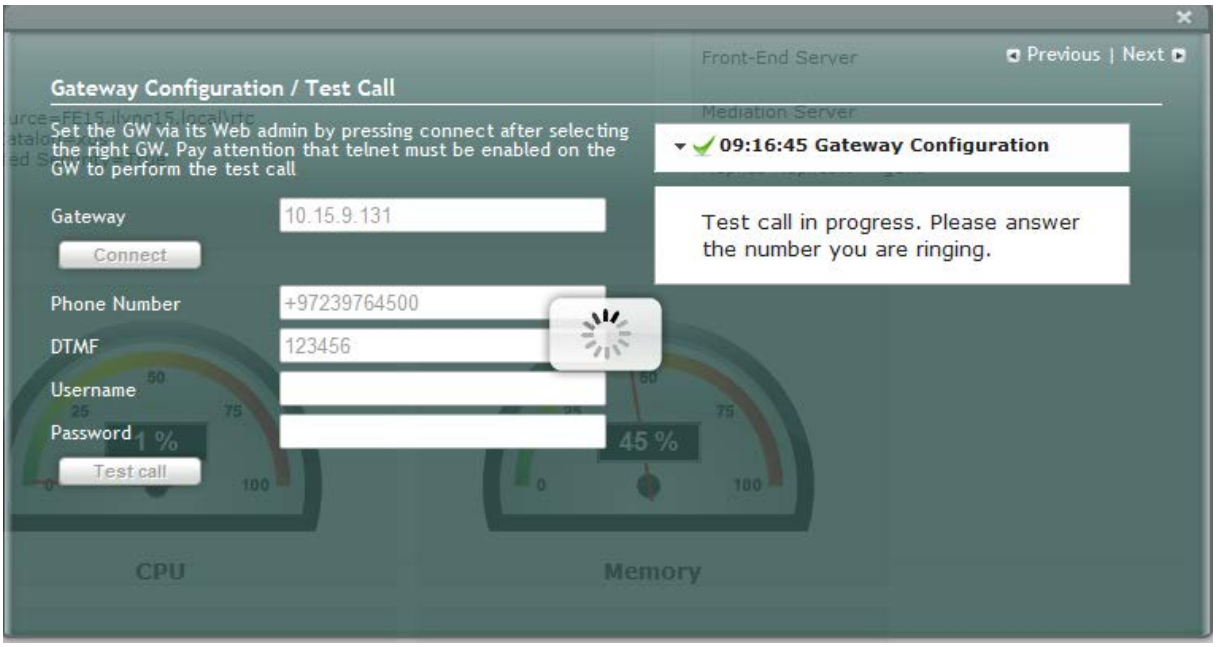
1. Enable Telnet on the PSTN Gateway, using the PSTN Gateway Web interface:
   a. Open the Telnet/SSH Settings page (**Configuration** tab > **System** menu > **Management** > **Telnet/SSH Settings**).
   b. From the 'Embedded Telnet Server' drop-down list, select **Enable Unsecured**.
   c. In the 'Telnet Server TCP Port' field, ensure that the port used for Telnet is '23' (default).

Figure 9-1: Enabling Telnet



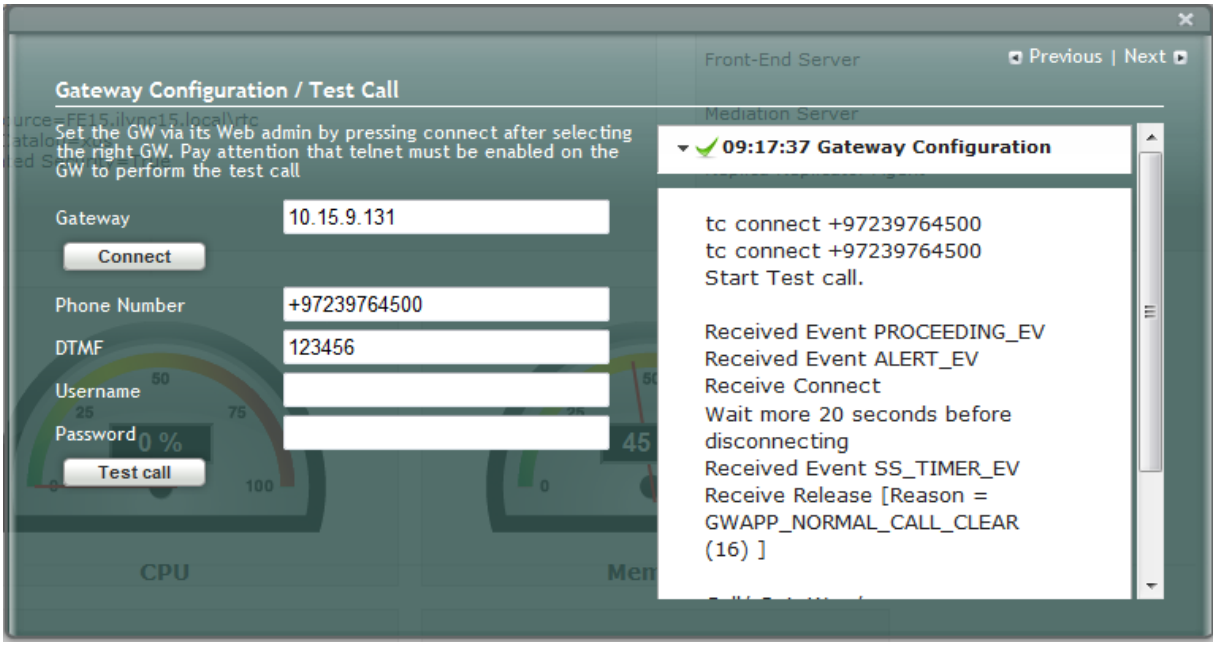
2. Establish a Telnet session with the PSTN Gateway.
3. Log in to the SBA Web Setup and do the following:
   a. Under the **Setup** menu, click the **Gateway Configuration** option.
   b. In the 'Gateway' field, enter the IP address or the FQDN of the gateway (as configured in Section 8.1 on page 102).
   c. In the 'Phone Number' field, enter a PSTN phone number.
   d. In the 'DTMF' field, enter any DTMF string. This DTMF string will be heard when the user picks up the phone handset (optional).
   e. If you changed the Web/Telnet login username and password of the PSTN Gateway, then enter their values in the 'Username' and 'Password' fields respectively; otherwise, leave the fields as is.
   f. Click **Test call**.

Figure 9-2: Gateway Configuration – Calling the Phone



If the phone does not ring, an error message is displayed and the call test fails. If the phone rings, lift the handset and confirm that you can hear the DTMFs. The following screen appears when you answer the phone:

Figure 9-3: Gateway Configuration – Call Answered



Note: It is recommended to disable Telnet after making the test call.

9.2 Testing Lync Calls

The **Lync Test Call** option allows you test a PSTN call initiated by the Lync Server 2013. The test call succeeds if the PSTN call is routed from Lync to the PSTN through the gateway.

9.2.1 Test Prerequisites

Before running the **Lync Test Call**, the following prerequisites must be met:

- Test users have been created in the Lync Server 2013 and are voice-enabled.
- VoIP Outbound Routing configuration has been setup and the correct policies have been assigned to the test users.
- Built-in-users for HealthMonitoring have been configured using the following commands:

  ```
  New-CsHealthMonitoringConfiguration -Identity
  <XdsGlobalRelativeIdentity> -FirstTestUserSipUri <String> -
  SecondTestUserSipUri <String>
  ```

  Where,

  - ***Identity*** is the FQDN of the pool where the health monitoring configuration settings are to be assigned (i.e., SBA FQDN).
  - ***FirstTestUserSipUri*** is the SIP address of the first test user to be configured for use by this collection of health monitoring settings. Note that the SIP address must include the sip: prefix, for example:

    ```
    -FirstTestUserSipUri sip:kenmyer@litwareinc.com
    ```
  - ***SecondTestUserSipUri*** is the SIP address of the second test user to be configured for use by this collection of health monitoring settings. Note that the SIP address must include the sip: prefix, for example:

    ```
    -SecondTestUserSipUri sip:jhaas@litwareinc.com
    ```

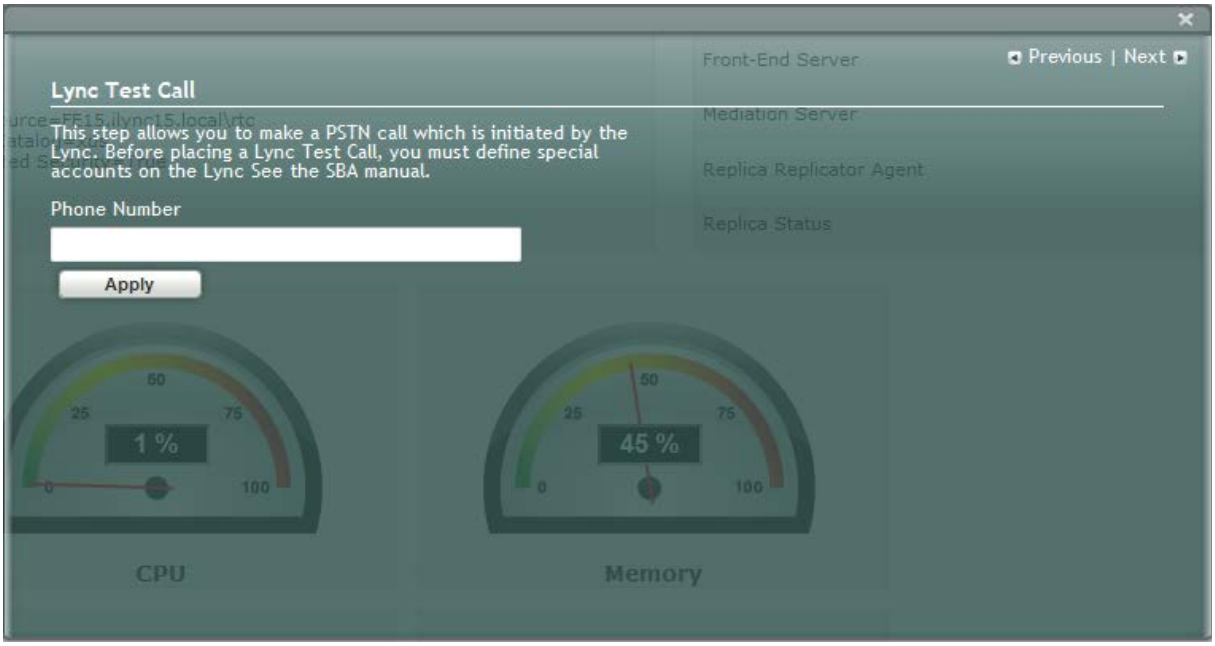
9.2.2 Running the Lync Call Test

The procedure for running the test is described below.

➢ **To run the Lync test call:**

1. Under the **Setup** menu, select the **Lync Test Call** option; the Lync Test Call screen appears:

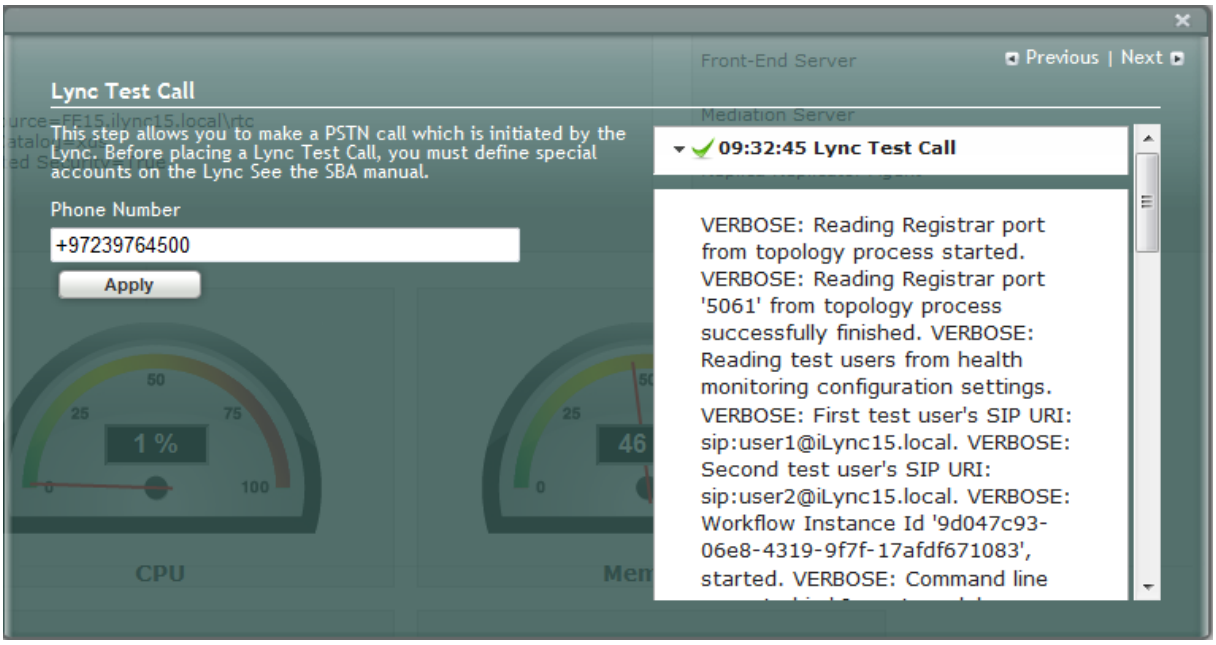
Figure 9-4: Lync Test Call Screen



2. In the 'Dial Check Phone Number' field, enter the PSTN phone number to dial.
3. Click **Apply** to start the test call.

If the test is successful, the phone of the PSTN user rings and when the handset is lifted, the DTMF tones are heard. If the phone does not ring, an error message is displayed on the screen. The screen displays logged details of the call:

Figure 9-5: Lync Test Call – Logged Call Test Result



Reader's Notes

10 Completing SBA Setup

Once you have completed all configurations as described in the previous sections, you need to perform the procedure described below to complete the SBA setup.

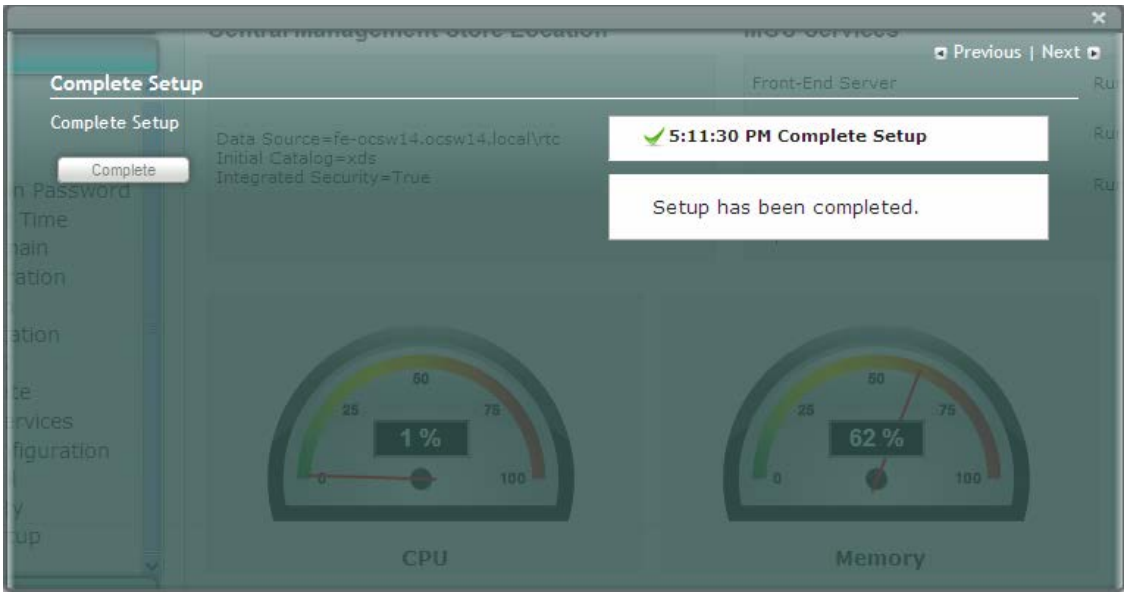
➢ **To complete SBA setup:**

1. Log in to the SBA Web wizard (if not logged in already).
2. Under the **Setup** menu, select the **Complete Setup** option; the Complete Setup screen appears:

Figure 10-1: Complete Setup Screen

3. Click **Complete**; the following screen appears, indicating that the SBA setup is complete:

Figure 10-2: Complete Setup – Setup Completed



A green check mark appears alongside the **Complete Setup** option under the **Setup** menu:

Figure 10-3: Complete Setup – Completed Successfully

11 Miscellaneous SBA Procedures

This section describes various procedures that can be done using the SBA Web-based tool.

11.1 Viewing General SBA Status in the Home Page

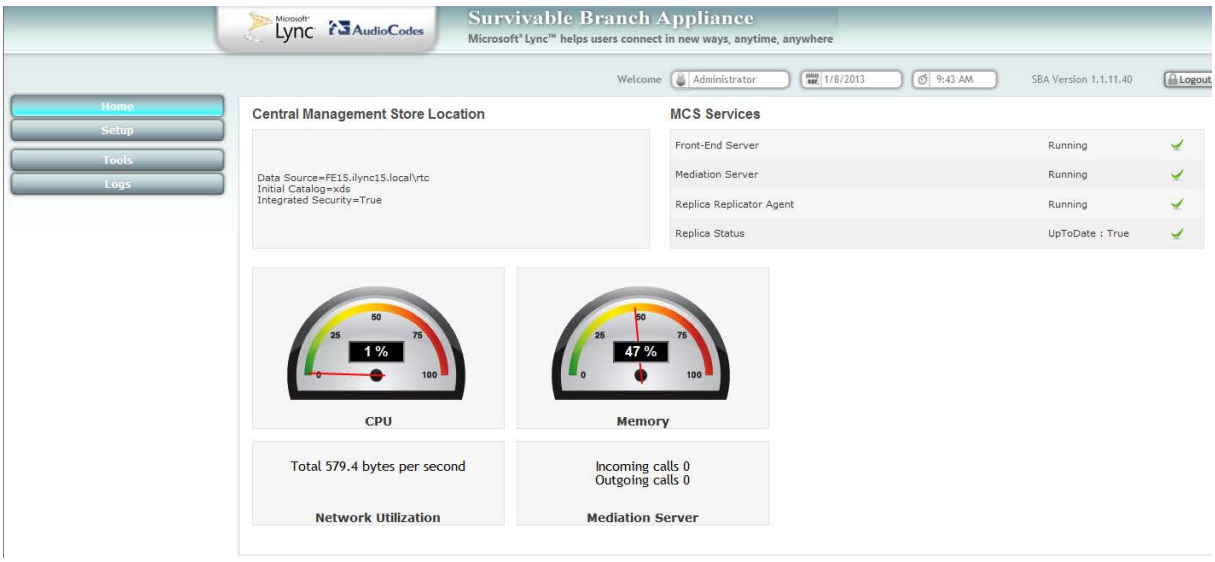
The general operating status of the SBA can be viewed in the Home page. This displays the following:

- Central management store location
- SBA services status (stopped or running)
- CPU, memory, and network usages
- Number of incoming and outgoing calls

➢ To view the Home page:

- Select the **Home** menu tab:

Figure 11-1: Home Page



11.2 Starting and Stopping SBA Services

You can stop and start SBA services as described in the procedure below.

➢ **To start and stop services:**

1. Select the **Tools** menu tab, and then click the **Start and Stop Service** option; the Start and Stop Service page appears:

Figure 11-2: Start and Stop Service Page

2. Click one of the following as required:
   - **Start All:** Starts the services on the SBA
   - **Stop All:** Stops the services on the SBA
   - **Restart Server:** Restarts the server
   - **Shutdown Server:** Shuts down the server

11.3 Updating System Components

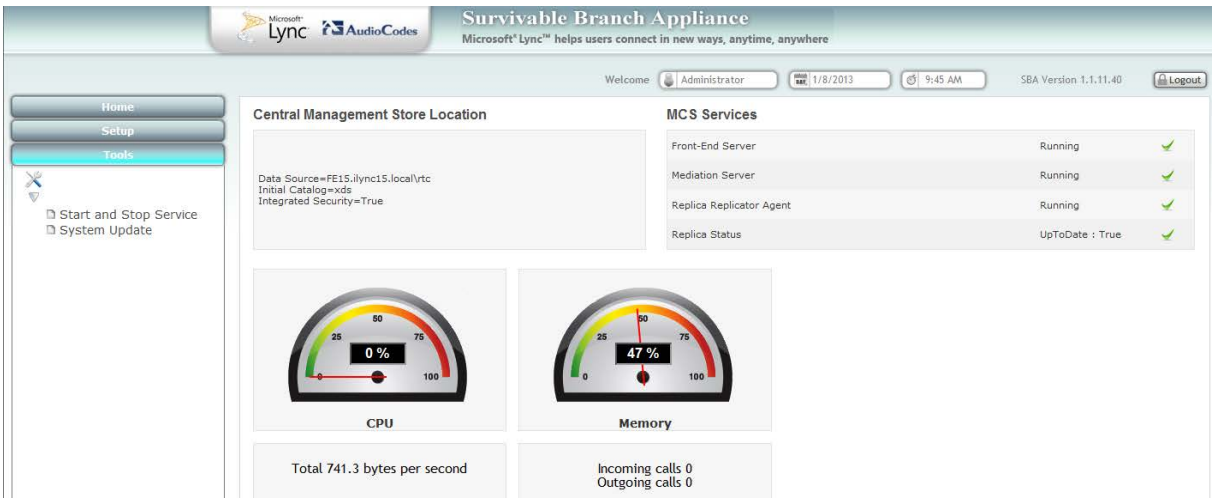
This section describes how to update system components using the SBA interface. The following components can be updated:

- SBA system components
- Microsoft system components

➢ **To update system components:**

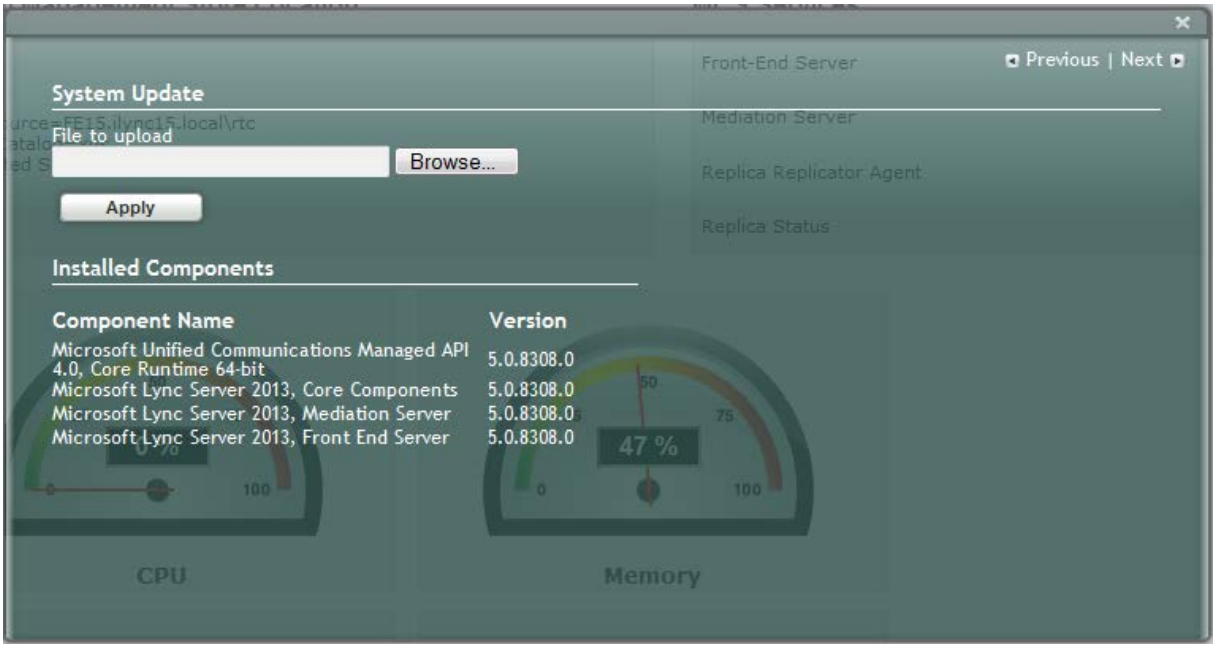
1. In the Tools menu, select the **System Update** checkbox.

Figure 11-3: Tools System Update Menu



The System Update screen is displayed:

Figure 11-4:System Update Screen

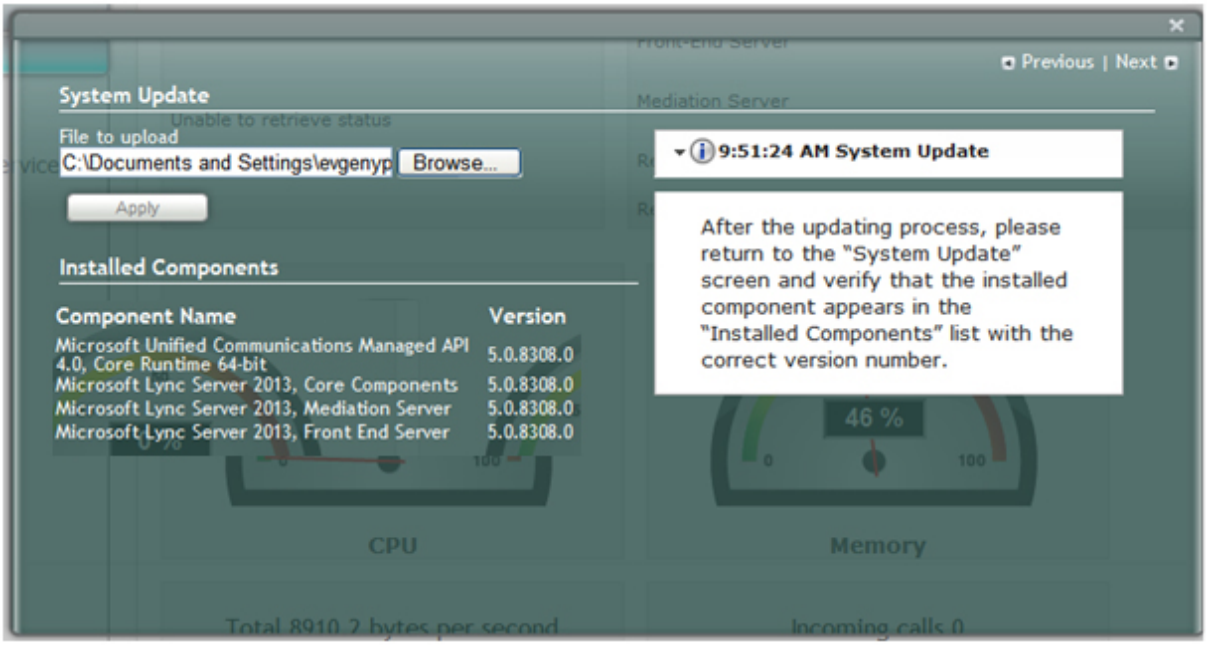


The currently installed Microsoft components are listed in the Installed Components pane.

2. In the 'File to upload' field, click **Browse** to select the file to upload and then click **Apply**.

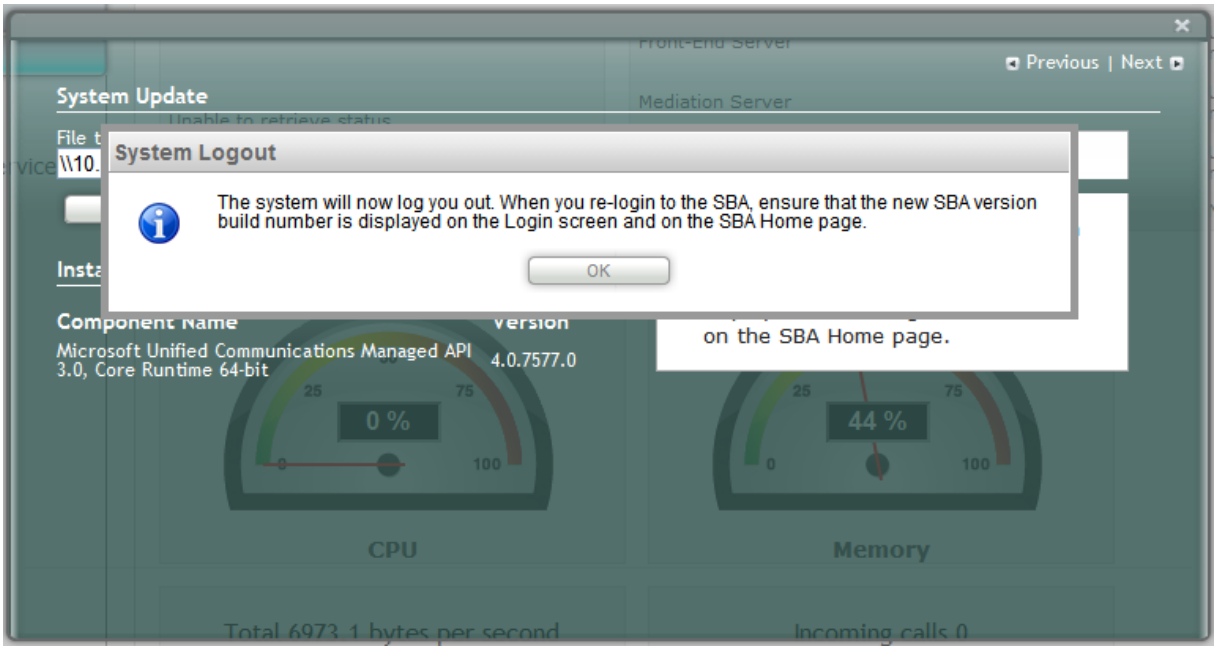
   If you are updating Microsoft system components, the following screen is displayed:

Figure 11-5:System Update Message-Microsoft System Components



If you are updating SBA system components, the following screen is displayed:

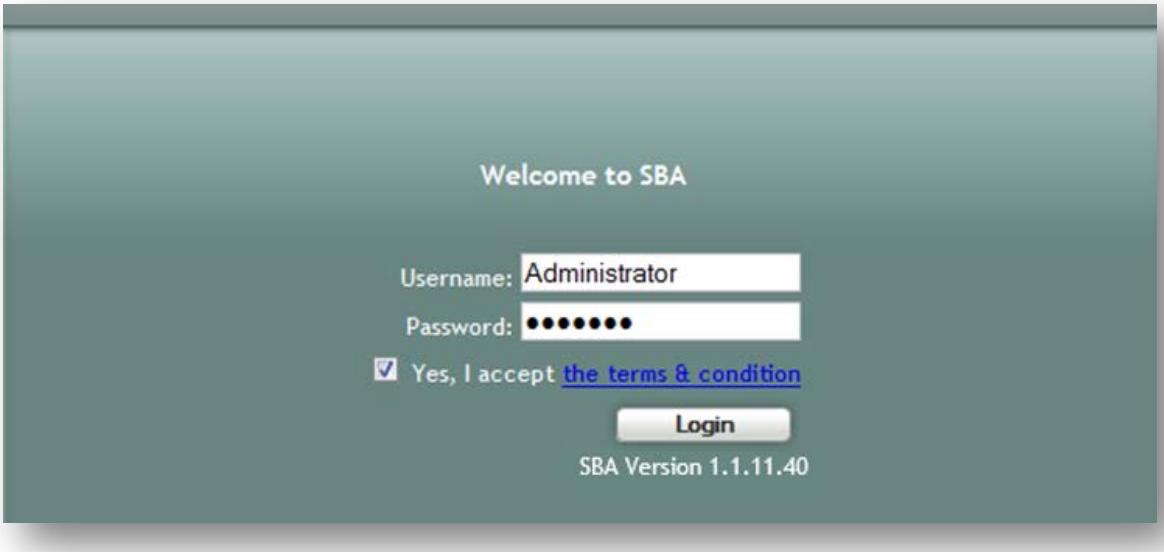
Figure 11-6: System Update Message-SBA System Components



In both cases, a time-stamp of the time that you commenced the System Update is displayed in the right-hand pane.

Wait a few minutes for the update to apply. At the end of the process, the System Logs out automatically and the login screen is displayed.

Figure 11-7: Login Screen after Automatic Log Out



3. Do one of the following:
   - If you are updating SBA system components:
     a. In the Login screen, verify that the new SBA version number is displayed (if it's not, see step 'd' below).
     b. Enter your login and password details, and if the Terms and Conditions checkbox is displayed, select it and then click **Login**.
     c. Ensure that the new SBA version number is displayed in the SBA Home Page.
     d. Logout and ensure that the new SBA version number is displayed in the Login screen.
   - If you are updating Microsoft system components:
     a. Enter your login and password details, and if the Terms and Conditions checkbox is displayed, select it and then click **Login**.
     b. In the Tools menu, select the **System Update** checkbox.
     c. Verify that the new component and respective version number is displayed in the Installed Components pane.

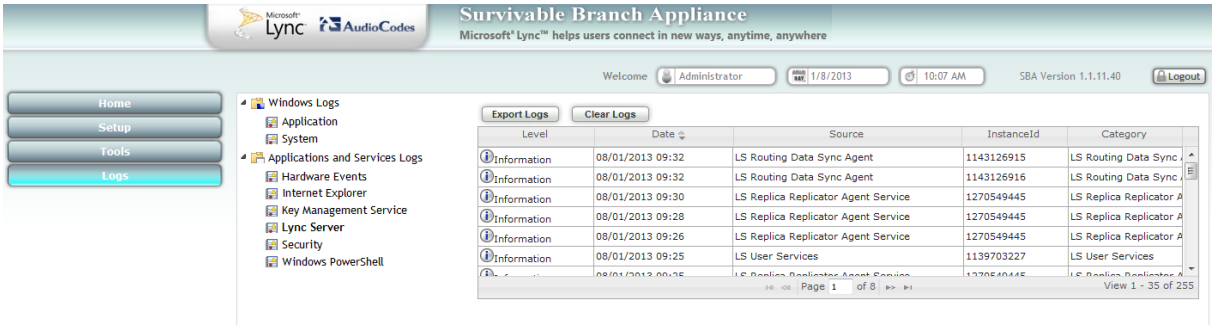
11.4 Viewing Logged Events

The procedure below describes how to view and handle logged events.

➢ **To view and handle logged events:**

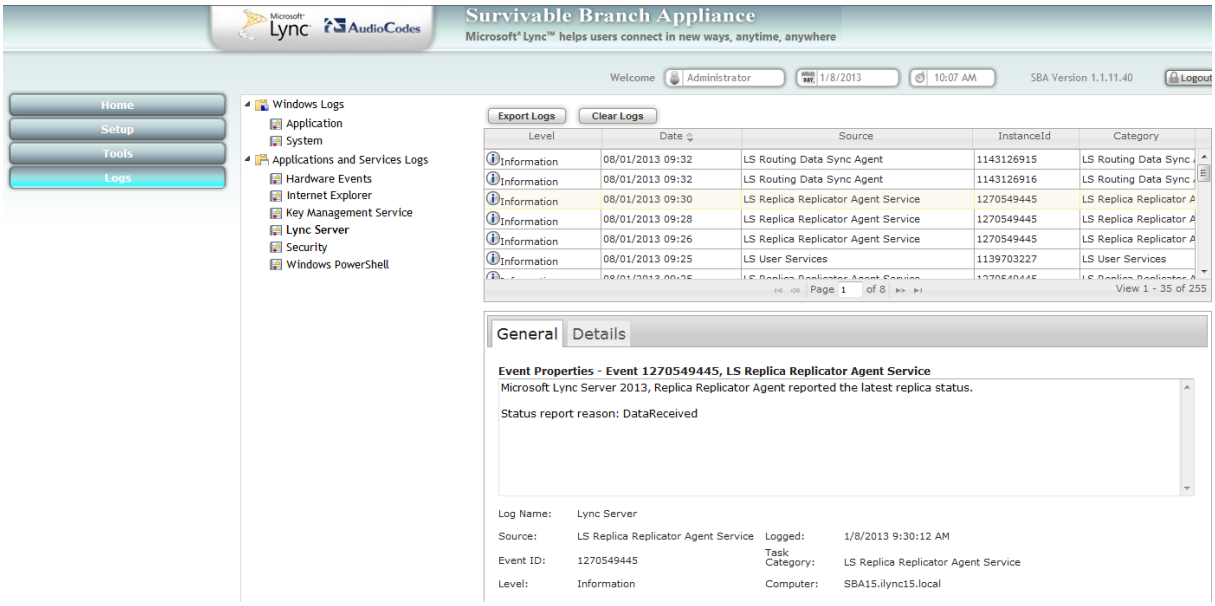
1. Select the **Logs** menu tab; the Logs screen appears displaying logged events:

Figure 11-8: Logs Screen Displaying Logged Events



2. To view details of a logged event, select the event.

Figure 11-9: Detailed Log Display



3. To clear the displayed log, click the **Clear Logs** button. To export the logged events, click the **Export Logs**.

11.5 Logging Out

The procedure below describes how to log out the SBA wizard.

➢ **To log out the SBA Web wizard:**

- Click the **Logout** button.

SBA Installation Manual

www.audiocodes.com